Cyber AI 4 Zero Trust Network Access

1 message

easytech4all tech <et4all.research@gmail.com> Wed, 24 Jan, 2024 at 5:00 am
Draft

GLOBAL CYBER INTELLIGENCE – CONSECRATED
Global Cyber Intelligence Consecrated . This Video Presentation is rededicated to the International Cyber Defense Umbrella comprising of Military Alliance Cyber Commands , Government and Federal Cyber Defense Agencies , Private CTI Defense Corporations , Security Operations Centre , Computer Emergency Response Teams , Transnational Independent Cyber Threat Intelligence Analysts & Specialists.

KEY HIGHLIGHTS –

UN , US , NATO , INDIA , Federal Security Agencies , Military Cyber Force and Commands , Private CTI Agencies and Corporations.

Two invaluable book recommendations from UN and suggestions to UN . My recent reads .

“The Basic facts about UN” is a mini encyclopaedia. Not just about UN but Copernican World Events and Crisis/Conflict response at the Macro Level including the development and progress of ICT’s and the ICT task force. The historical significance and evolution on a chronological linear timeline. Also quite significant was the section on Peaceful use of outer space – Relevant Treaties and Agreements. UNISPACE conferences , cooperation with European Space Agency (ESA) , NASA , International Astronautical Federation (IAF) , Committee on Earth observation satellites (CEOS) , Committee on Space Research (COSPAR) etc.

The other Book uncommon opportunities – Agenda for Peace and Equitable development
The Report of the International Commission on Peace and Food by International Center for Peace and Development USA and M.S. Swaminathan Research Foundation Chennai India .
Highlights are the sections on the “Peace Imperative” – Information Superhighways , War as an instrument of Policy , Nuclear Weapons (START 1 , START 2 , NPT , CTBT , Ballistic Missiles) , Confidential Studies by NATO , Cooperative Security, MAD doctrine , World Army Proposition and Hypothesis etc . Alacritous rise of India and China in the Global Order and what made it possible.

US Cyber Policy for Deterrence. Executive Order 14028 Improving the Nation’s cybersecurity. This EO Mandates endpoint protection , defining logging requirements , implementing audit logging in a unified way and enhancing the capabilities to provide further insight into system and account actions. The EO responds to an increase in Cyberattacks that use ransomware to cripple critical infrastructure components related to National Security and the public . Enhancing existing information assurance security controls as a part of a Risk management framework is a suitable mechanism to facilitate compliance and justify funding based on these Presidential requirements.

White House Cyber Physical Resilience Initiative (ISSA SIG) – Cyber Resilience refers to the ability to protect electronic data and systems from cyberattacks as well as to resume business operations quickly in case of a successful attack. In times of increasing damage and sophistication of attacks it is of paramount importance to develop critical cyber resilience capabilities in each organisation. Yet cyber resilience is currently understood differently by various organisations despite the fact that NIST had published clear guidelines(800-160) then followed by other valuable publications and initiatives from MITRE , CERT -US , CISA etc.

NATO CCDCOE Locked Shields Livefire Exercise 2023 – a unique international Cyberdefence Exercise offering the most complex technical live fire challenge in the World. From a Strategic perspective the exercise offers training and practice in effective decision making and crisis coordination when facing large scale cyber attacks targeting the critical sectors and it’s infrastructure. NATO Cyber Commanders Handbook 2.0 at stakeholders meeting in Tallinn Estonia – leveraging a cooperative approach for Cyber Defence.

India’s meteoric rise in United Nations Specialised Agency for Information and Communication Technologies – International Telecommunication Union (ITU) ranking for everything Cybersec . Ranked at 10th from the 47th Spot with an overall Score of 97.49. 4th Spot in Asia Pacific Region.

USA and UK ranked First and Second respectively. Saudi Arabia and Estonia was ranked third. South Korea , Singapore , Spain shared the fourth spot . Russia , UAE , Malaysia shared the Fifth Spot . Lithuania came in sixth followed by Japan , Canada , France at seventh , eight and ninth respectively.
Also 3 Indian Leaders have been named in Global Hall of Fame report that identified “CLOUD SECURITY AS THE BIGGEST CHALLENGE” – Indian Govt once said that they want to make INDIA the Global hub for Cybersecurity. And India is indeed making some good progress in that much needed direction . As a fast growing “World Class Digital Payment Ecosystem” economy – Cybersecurity and Cyber Resiliency become of paramount importance mechanically.

Open Source Software is India’s inherent Strength . A Quick analysis of the Internet and YouTube will reveal India’s talent in Open Source OS Linux distros – Ubuntu , Fedora , Kali Linux , Elementary OS , Debian etc . DIY’s and How 2 Do’s across the length and

breadth of the Internet unveil this hidden untapped and unorganised skill set that needs to be developed and promoted further . The Beauty of OSS are the following.

Right to use study change distribute the software and its source code to anyone for any purpose.

Development in Collaborative Public Manner.

Examine the Code thereby facilitating public trust in the Software.

Linux has the largest installed base of all general purpose operating systems (including AOSP and ChromeOS) . From running the terminals at the International Space Station to some of the fastest supercomputers..OSS is everywhere.
The Chromebook, which runs the Linux kernel-based ChromeOS, dominates the US K–12 education market and represents nearly 20 percent of sub-$300 notebook sales in the US. Linux is the leading operating system on servers (over 96.4% of the top 1 million web servers' operating systems are Linux), leads other big iron systems such as mainframe computers, and is the only OS used on TOP500 supercomputers (since November 2017, having gradually eliminated all competitors).

Linux also runs on embedded systems, i.e. devices whose operating system is typically built into the firmware and is highly tailored to the system. This includes routers, automation controls, smart home devices, video game consoles, televisions (Samsung and LG Smart TVs use Tizen and WebOS, respectively), automobiles (Tesla, Audi, Mercedes-Benz, Hyundai, and Toyota all rely on Linux), spacecraft (Falcon 9's and Dragon 2's avionics use a customized version

More Snapshots in the above video presentation.

Future of the Intelligence Community Workforce – Enabling a Secure Hybrid Work Environment – CIA and MITRE Corp.

US Cert (Computer Emergency Response Teams) , Cybersecurity and Infrastructure Security Agency (CISA) National Security Agency (NSA) Events .

Intelligence and National Security Alliance (INSA) and ISSA (Information Systems Security Association) Brainstorms Webinars Seminars .

. EU Cyber Defence Innovation Program.

European Cyber Agora.

National Cyber Strategies to Defend Critical Infrastructure.

Global Annual Cybersecurity Summits and National Cybersecurity Alliance endeavours.

UKCSA UKSec – Challenges faced by Governments and International Law Enforcement.

. Cybersecurity Projections and Predictions.

Cyber Task Force – FBI Criminal Cyber Squad .

Cyber World Congress – 24 hr Virtual Events.

. Cyber Threat Intelligence Talks.

. CyberAI and its impact on OSINT.

Cyber Intelligence Units Quarterly Updates (Infoblox)

CYBERWARFARE PREPAREDNESS by Allen Ari Dziwa.

Military Cyber Commands and Cyber Force (SoC- Trident Jaguar)

Assessing the risk and Protecting the Supply Chain.

. Podcast on Cyberweapons.

. Future of Cybersecurity and Risk Analysis.

Cyber Threat Intelligence and Incident Response.

Cybersecurity Advanced Persistent threat Defenders Overview.

. Virtual Intelligent Automation Exchange – Director of AI Defense Intelligence Agency (DIA)

. Small Business National Security Showcase (Directorate of Digital Innovation CIA)

. CISO perspective – Delta Airlines.

. Cyber Strategies for a World at War (Open Source Aggregation and Analysis).

. WEF and INTERPOLs Global Risk Annual Assessments and SOC – Cyber Ploygon.

Google Cloud Security talks and threat Analysis Group.

Digital Risk Management e-learning platform for mediators. UN DPPA and Cyberpeace Institute.

1PowerCyber @ Easytech4all CTI Research & Analysis consultancy focuses it's energies on Military Cyber Commands and Global Federal Agencies CTI reports , webinars , brainstorms , bright talks by global industry and Agency experts to build a threat Intel knowledge pool . The Cyber Threat Intel Knowledge pool in turn takes shape of mindmaps , infographics and video content presentations to be used for Blogs , Digital Magazines , Newsletters and CMS .

This Knowledge pool also facilitates analysis and benchmarking of EDR/NDR , Siem , SOAR solutions available for different ecosystems . This coupled with OSINT research conducted through different search engine Algorithms facilitates proactive Cyber Threat Intelligence Projections incorporating various Geopolitical , Strategic and Policy inputs. Eventually this threat Intel gets included on Collaborative CMS & services integration platform.

Cyber Strategic Communication based on OSINT and Global Cyber Policy Analysis also remains an area of Major interest as it is indispensable for future Cyber threat projections.

OS Hardening – Mapping Desktop / Mobile OS and Application Security with every successive firmware and security patch is continuous work in progress at the Threat Intel Research Consultancy.

This Video Presentation is a succinct snapshot of some Preliminary and detailed experience with Global Cyber Intelligence Think Tanks , Organizations and Associations .

From Researching Analysing Cybersecurity and CTI Products/Services to functioning as a Cyber Threat Intel Provider for Governments , Global Agencies and CTI Organisations. The Scope for Transnational Cyber Alliance remains stupendous.

1Power Easytech4all Cyber threat Intelligence Solution primarily relies on the Cyber Prudence and Strategic Insights of Global Experts from UN Cyber Policy Assessments and Debates on ICT's , White House Cyber Policy EO's , Risk Assessments , White House Cyber Resilience Initiatives through various organisational SIGs etc . Also ISSA , INSA ,NATO , UNIDIR , European Defence Agency (EDA) , National Security Agency (NSA) , Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) , World Economic Forums (WEF) Annual Critical Risk Assessments and Cyber Polygons (SOCs) in addition to Pvt Agency Security Operations Centers findings plus CTI analysis.

They are the Cyber beacons for the World shaping Global Cyber Policy and Cyber Deterrence Countermeasures plus standards .

1PowerCyber @ easytech4all.net

https://1powercyber.substack.com

https://1powercyber.blogspot.com

https://easytech4all.tumblr.com

https://linktr.ee/1powercyber

The policy challenges presented by cyberspace are not solely technological in nature. The cyber domain is a human-made environment and is fundamentally shaped by human behaviour. It amplifies such behaviours for better or worse, the impacts of which are usually also felt in the physical world. Cyberspace is owned and operated by private companies, governments, non-profit organisations, individual citizens and even criminals. This means that any strategic response to this context must link geostrategy and national security, criminal justice and civil regulation, economic and industrial policy and requires a deep understanding of the different cultural or social contexts and value systems interacting online.

Cyberspace also transcends national borders. Technology supply chains and critical dependencies are increasingly global, cyber criminals and state-based actors operate from

around the world, powerful technology companies export products and set their standards, and the rules and norms governing cyberspace and the internet are decided in international fora. Cyberspace is also continually evolving as technology and the ways people use it change, requiring us to adopt an agile and responsive approach.

What is cyberspace?

To many of us, cyberspace is the virtual world we experience when we go online to communicate, work and conduct everyday tasks. In technical terms, cyberspace is the interdependent network of information technology that includes the internet, telecommunications networks, computer systems and internet-connected devices. For the military, and when considering our efforts to counter threats in cyberspace, it is an operational domain, along with land, sea, air and space.

How is cyberspace experienced?

Cyberspace is, by definition, a 'shared' space and its scale and complexity means that every person's experience of it is unique. Citizens access cyberspace when they check their bank accounts online or stream a film at home. Businesses use cyberspace to connect their staff with the resources they need, whether this is access to information or control over a manufacturing process. Governments provide public services to their citizens using online portals. Cyber professionals look 'under the hood' at the technology, standards and protocols that make it all 'just work' for users. All these groups use cyberspace in different ways and for different purposes, and we are all making an ever-greater use of it.

Cyberspace can be described in terms of three layers:

Virtual

The part of cyberspace most people experience. It consists of representations of people and organisations through a virtual identity in a shared virtual space. Virtual representations could be an email address, user identification, a social media account or an alias. One person or one organisation can have multiple identities online. Conversely, multiple people or organisations could also create just a single, shared identity.

Logical

The part of cyberspace made up of code or data, such as operating systems, protocols, applications and other software. The logical layer cannot function without the physical layer and information flows through wired networks or the electromagnetic spectrum. The logical layer, along with the physical layer, allows virtual identities to communicate and act.

Physical

The physical layer of cyberspace includes all the hardware on which data is transmitted, from the routers, wires and hubs that you have in your home, to large complex telecommunications systems operated by big tech companies. As well as physical infrastructure it includes the electromagnetic spectrum on which data is transmitted, such as WiFi and radio.

Cyber attacks can have devastating consequences for both companies and their customers. Network compromise can lead to unauthorized access to and theft of both business and customer data. In 2022 in the US alone, there were 1,802 recorded data compromises, with 422.14 million people affected by said compromises.

Manage cyber
security risk

In order to manage cyber security risk, government organisations must be able to identify, assess and understand them. The foundation of this lies in the visibility and understanding of assets, their vulnerabilities, and the threat to them – whether internal to an organisation or emanating from its supply chain. Clear accountability and robust assurance will ensure that risk owners are aware of the risks they have the responsibility to manage, and that they are doing so appropriately.

Information about vulnerabilities must be shared across governments to provide a central view of critical vulnerabilities that will enable cross-government risks to be identified and managed, facilitating rapid assessment, coordination and mitigation at scale.

Protect against
cyber attack

The protective stance of individual government organisations will be inextricably linked to their assessment and management of risk. While it will never be possible to protect against all attacks, those accountable must be able to demonstrate that they have appropriately considered those risks and responded accordingly.

Proportionate cyber security measures must be embedded in the technology government uses, and technology and digital services will be correctly designed, configured and managed. Crucially, governments must develop its shared capabilities, tools and services to address common cyber security issues at scale, improving cyber security across the whole of government as well as driving efficiency and value for money.

3.At the heart of any government's responsibility must be to protect the data it handles. As well as appropriately classifying information, governments must handle and share it in a way that is commensurate with the risks it presents, using the appropriate IT Systems.

Detect cyber
security events

Building on the foundation of risk management and commensurate protective measures, governments must develop its capability to detect cyber security events across every part of its estate to ensure that risks can be mitigated before they critically impact government functions and services.

This means having the capability to monitor systems, networks and services to detect cyber security events before they become incidents. Enhanced coordination will enable governments to have the agility to use these data inputs to detect at pace and scale, facilitating coherent responses as well as providing the capabilities to detect more sophisticated attacks.

Minimise the impact of cyber security incidents

While effective risk management, appropriate and proportionate protective measures and enhanced detection capability will make governments a considerably hardened target, government organisations will still be impacted by cyber security incidents.

Governments must therefore be fully prepared and able to respond to cyber incidents with the capability to restore affected systems and assets and resume the operation of its functions and services with minimal disruption. A critical component of this will be establishing the mechanisms to test and exercise incident response plans, both organisationally and across government, as well as the ability to learn lessons from incidents and 'near misses'.

Cyber Critical Infrastructure | Nuclear impingement

CCI | Nuclear Reimagined

CCI Infra – Nuclear Landscape | NCAM 2022

Role of Dynamic Multidimensional Security Approach Zero Trust Network Access on Critical Infrastructure.

Cyber Attacks on Critical Infrastructure | NATO

Zero Trust Architectured Networks – US Cybersecurity and Infrastructure Security Agency . Department of Homeland Security

US Intelligence and National Security Alliance

Protecting Critical Infrastructure: Key Elements of the New National Cybersecurity Strategy

Tuesday, May 2 | 1:00 – 2:30 PM ET | Virtual – two-part program!

Panelists:

Brian Scott, Deputy Assistant National Cyber Director for Cyber Policy and Programs, Office of the National Cyber Director, Executive Office of the President

Speaker from CISA (Invited)

Chris Boyer, Executive Committee Member, Communications Sector Coordinating Council, and VP, Global Security and Technology Policy, AT&T

Amanda Craig, Executive Committee Member, IT Sector Coordinating Council and Senior Director, Global Cybersecurity Policy, Microsoft

Matthew Eggers, VP for Cybersecurity Policy, U.S. Chamber of Commerce

https://insaonline.us8.list-manage.com/track/click?u=2bbe7114be6cc1ae543a8f374&id=4f659e75a0&e=d386303ff8

Cyber Council – New White Paper

Industry Contributions to Offensive Cyber Operations, outlines the importance of public/private collaboration in cybersecurity and provides five key recommendations that can help strengthen U.S. critical infrastructure.

https://insaonline.us8.list-manage.com/track/click?u=2bbe7114be6cc1ae543a8f374&id=aa1dc2fed6&e=d386303ff8

Key Highlights of
Google Cloud Security – 2023 Outlook

https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-1

Frontline Threat Intel Panel

https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-2

Cyber Crime Metamorphosis: A Case Study Examining How Criminals Adapt to Chaos

https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-3

Managing Open Source Software Security

https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-4

DDoS Trends at US Elections and What's New with Cloud Armor

https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-5

Defeating Cryptomining Attacks with Native Security Controls

https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-6

Cloud Detection & Response Survey: Challenges and Insights

https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-7

Office of the CISO
RESOURCES

Improve Decision Making with Automated Contextual Awareness

https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-8

Quick recap of Global Cyber Threat Intelligence brainstorms (2019-2022) by https://1Power.substack.com and https://easytech4all.net

US Federal Agencies. Security Organisations
US Cyber Command.NSA.US Dept of Homeland Security.Department of Defense . Secret Service CID. CISA.FBI

https://1powercyber.blogspot.com/2022/05/us-cybersecurity-global-conference.html?utm_source=pocket_mylist

UN Security Council Cyber Threats Debate –

UNIDIR Cyber Stability Conference 2021 & AI Disruption Peace Security (innovations dialogue) 2022

https://1powercyber.substack.com/p/unidir-cyber-stability-conference

Importance of Information and Communication technologies .

NATO Locked Shields 2022

https://1powercyber.substack.com/p/nato-locked-shields-2022?utm_source=pocket_mylist

Cyber Polygon with World Economic Forum and INTERPOL

https://1powercyber.substack.com/p/wef-and-interpol-cybersecurity-mega?utm_source=pocket_mylist

White House National Cybersecurity Strategy

https://www.csoonline.com/article/3689911/white-house-releases-an-ambitious-national-cybersecurity-strategy.html

Countering Ransomware with Department of Homeland Security , Cybersecurity and infrastructure Security Agency , Federal Bureau of Investigation , SecretService Criminal Investigation Department

Cyber Essentials by Cybersecurity and Infrastructure Security Agency and Department of Homeland Security.

Ransomware Attackers Defenders – FBI's perspective

US Cyberspace Solarium Commission

UK Cybersecurity Association with Digital Police Center.

Fourth Annual Cybersecurity Summit by Cybersecurity and Infrastructure Security Agency .

Fourth CEO Summit – USA

State of American Business 2023

Challenges faced by Government and international LAW Enforcement

Intelligence and National Security Alliance (INSA) 2022 UPDATE

What is Advanced Cyber Threat Intelligence ?

Accreditations Webinars LMS – Cybersec CTI

Google Cloud Security Summit with Chris Inglis (National Cyber Director , Executive office of the US President)

https://1powercyber.substack.com/p/google-cloud-security-summit-with

Security information and event management (SIEM) is a field within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware. Vendors sell SIEM as software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes. The term and the initialism SIEM was coined by Mark Nicolett and Amrit Williams of Gartner in 2005.

https://1powercyber.substack.com/p/security-information-and-event-management?utm_source=pocket_mylist

Zero Trust Architectured Networks by Cybersecurity and Infrastructure Security Agency

1PowerCyber and Easytech4all Global CTI Research & Analysis.

Mapping Global CTI Landscape and Visual Trends

International Cyber Threat Intelligence Brainstorms

Safe and Secure Digital Ecosystem for Schools by US Department of Homeland Security and Department of Justice

Global Cyber Threat Landscape

CyberKinetic and 5G

https://1powercyber.blogspot.com/2022/05/cyber-kinetic-world-war-3-and-5g-in.html?utm_source=pocket_mylist

https://1powercyber.substack.com/p/cyber-kinetic-warfare?utm_source=pocket_mylist

Cyber Independence and Freedom

Cyberattacks and Critical Infrastructure (Reading & Resources)

Space Threats and Satellite Navigation Systems

https://1powercyber.substack.com/p/space-threats-satellite-navigation?utm_source=pocket_mylist

Comsec Protocols and Paradigms

https://1powercyber.substack.com/p/comsec-protocols-and-paradigms?utm_source=pocket_mylist

Advanced Cyber Threat Intelligence Landscape and Updates via Digital Magazine by 1PowerCyber for Easytech4all.net

https://bit.ly/3P8gCTT

Advanced Cyber Threat Intelligence Research Analysis Assessment and Projections . Video Playlist .

https://bit.ly/3yqDEje

Advanced Cyber Defense Threat Intelligence Blog in Progress

https://easytech4all.net/author/easytechonline/

https://1powercyber.substack.com

https://1powercyber.blogspot.com

https://easytech4all.tumblr.com/

References

Clarke R.A, K. R. (2010). Cyber war: the next threat to national. eCCO.

Clarke, R. (2011). Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins.

Cybersecurity and Infrastructure Agency. (2021, October 15). CISA HOME. Retrieved October 14, 2021, from https://www.cisa.gov/about-cisa

Gazula, M. B. (2017). Cyber Warfare Conflict Analysis and Case Studies. Massachusetts Institute of Technology .

Jeremy Rabkin, A. R. (2016). Hacking Back Without Cracking Up. Aegis Paper Series No. 1606.

Kukuh Ugie Sembodho, A. T. (2021). The Limitation of United States Deterrence Strategy Towards North Korean Cyber . Global Strategis, p. 150.

Libicki, M. (2009). Cyberdeterrence and cyberwar. Santa Monica: The Rand Corporation.

M, T. (2012). An analysis for a just cyber warfare in Cyber Conflict (CY-CON). , 2012 4th International Conference on,, (pp. 1-10).

National Security Agency. (2021, October

14). NSA Home.

Parks R, D. D. (2011). Principles of cyberwarfare, security privacy. IEEE, 30-35.

Rid, T. (2012, March). Think Again: Cyberwar. Foreign Policy , pp. 80-84.

Sanger, D. (n.d.). The Perfect Weapon: War, Sabatoge, and Fear in the Cyber Age. New York: Crown Publishers.

Schmitt, M. (2014). The Law of Cyber Warfare: Quo Vadis? Stanford Law & Policy Review, 269-270.

Tallin Mannual. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

The White House. (2011, April). National Strategy for Trusted Identities in

Cyberspace.

The White House. (2021). Improving the Nation's Cybersecurity. Federal Register Vol. 86.

Trautman, L. J. (2016, April). Cybersecurity: What About US Policy? Journal of Law, Technology & Policy, p. 344.

US Cyber Command. (2021). US Cyber Command Mission. Retrieved from https://www.cybercom.mil/About/Mission-and-Vision/

The dramatic surge in open source software supply chain attacks has sent defenders scrambling to find mitigations and solutions.

Software supply chain attacks increased by 742% at a time when we depend on open source software to build 97% of all enterprise code.

Security debt is a real problem for most organizations in the world today and the attackers will utilize this to their advantage. The more vulnerabilities a company has, the more likely it is that a malicious actor will take advantage of them. Security debt increases the risk of hackers gaining access to a company's network, meaning the risk of a potential data breach soars.

To prevent security debt from building up, defenders must keep system hygiene front of mind and focus on proper network zone segmentation, essentially building a zero-trust networks.

Distributed denial of service attacks, or DDoS attacks, see malicious actors attempt to disrupt a site by overwhelming its infrastructure with a large amount of internet traffic. As DDoS attacks overwhelm a site's bandwidth, this prevents users from accessing it.

Cloudflare Blocks Record DDoS Attack as Threats Surge

The attacks, which originated from more than 30,000 different IP addresses, targeted websites including a gaming provider, cryptocurrency companies, hosting providers, and cloud computing platforms

In today's interconnected world, critical infrastructure is under constant threat from cyberattacks that can compromise the availability, integrity, and confidentiality of essential systems and services. As a result, governments around the world are implementing regulations to protect these vital assets from harm.

With a predicted 25.4 billion active Internet of Things (IoT) devices worldwide in 2030, companies should be looking to protect it as a rapidly growing asset and target for cyber attacks.

Research by Nozomi Networks Labs for its OT/IoT security report has found that in the latter half of 2022, IoT devices were frequently targeted by malicious actors aiming to gain control of them. Likewise, Operational Technology (OT) systems were a similar target due to their ability to destabilize a company's network.

The ever-present threats of ransomware and data breaches make it imperative to lock down systems and prevent attackers from gaining a foothold. Hardening a system means reducing its attack surface and implementing defence in depth, preventing an entire system compromise.

The Domain Name System (DNS) is one of the oldest internet infrastructures, and often overlooked in security. However, through it passes an incredible amount of attack traffic. Attackers often use DNS to conduct command and control (C2) communication, download malware onto a machine, and facilitate multistage attacks.

State of the Internet (SOTI) report to gain insights into malicious DNS traffic and its potential impact: By Akamai.

26% of infected devices have reached out to identified initial access broker (IAB) C2 domains, including Emotet- and QakBot-related domains.

IABs present a large risk to organizations, as their primary role is to do the initial breach and sell access to ransomware groups and other cybercriminal groups.

30% of affected organizations are in the manufacturing sector — twice as many as the second-largest vertical.

Network-attached storage (NAS) devices are ripe for exploitation, as they are less likely to be patched and hold troves of valuable data. Our data shows attackers are abusing these devices through QSnatch.

Malware is a fast-growing, ever-evolving threat to cyber security. In the first six months of 2022, over 2.8 billion malware attacks were reported worldwide. Beyond risks to their network, malware like ransomware can have real, monetary costs for businesses. In 2021, damages of ransomware alone cost US$20bn. This was a 6054 percent increase on the global cost of ransomware in 2015, which was $325mn.

CLOUD SECURITY.

"Cybersecurity remains at the top of every organisation’s agenda. Google Cloud’s unique capabilities and expertise can help organisations, large and small, in the public or private sector, address today’s most prominent security challenges and imperatives:

* Zero Trust

* Securing the Software Supply Chain

* Ransomware and other emerging threats

* Cloud governance and Digital Sovereignty

Whether you use our trusted cloud for digital transformation, or continue to operate on-premise or in other clouds, you’ll learn how we can help you be safer with Google."

https://cloudonair.withgoogle.com/events/summit-emea-security-2022#:~:text=Cybersecurity%20remains%20at,safer%20with%20Google.

Complete End to End Cyber Threat Intelligence Solution - Virustotal + Chronicle + Siemplify

The U.S. government has improved its alert process for emerging cyberthreats to the United States and its allies and partners around the world—with the U.S. Computer Emergency Response Team (US-CERT) alert system and the MITRE ATT&CK framework at the center. In response to a new threat, US-CERT uses MITRE ATT&CK to describe observed adversarial tactics, techniques, and procedures (TTPs).

Describing adversary behavior using the CTI knowledge base is a cornerstone of the threat-informed defense paradigm. Techniques rarely occur in isolation, and instead, the attacker typically uses each technique to pave the way for others as they pursue their ultimate objectives.

Emotet continues to be used in wide broad-based attacks against victims in all sectors across the world.

The infamous botnet has been disrupted thanks to an international effort across the US, Canada, and several European nations.

Quick recap of Global Cyber Threat Intelligence brainstorms (2019-2022) by https://1Power.substack.com and https://easytech4all.net

US Federal Agencies. Security Organisations

US Cyber Command.NSA.US Dept of Homeland Security.Department of Defense . Secret Service CID. CISA.FBI

https://easytech4all.net/cyber-conference/

https://1powercyber.blogspot.com/2022/05/us-cybersecurity-global-conference.html?utm_source=pocket_mylist

UN Security Council Cyber Threats Debate -

https://easytech4all.net/2022/03/06/un-security-council-cyberthreats-debate/

UNIDIR Cyber Stability Conference 2021 & AI Disruption Peace Security (innovations dialogue) 2022

https://easytech4all.net/2022/07/05/unidir-cyber-stability-conference-3rd-december-friday-2021/

https://1powercyber.substack.com/p/unidir-cyber-stability-conference

Importance of Information and Communication technologies .

https://easytech4all.net/2022/02/05/unidir-ict-information-communication-technologies/

NATO Locked Shields 2022

https://1powercyber.substack.com/p/nato-locked-shields-2022?utm_source=pocket_mylist

Cyber Polygon with World Economic Forum and INTERPOL

https://easytech4all.net/2022/01/16/cyber-polygon-2020-2021-and-2022/

https://1powercyber.substack.com/p/wef-and-interpol-cybersecurity-mega?utm_source=pocket_mylist

White House National Cybersecurity Strategy

https://www.csoonline.com/article/3689911/white-house-releases-an-ambitious-national-cybersecurity-strategy.html

Countering Ransomware with Department of Homeland Security , Cybersecurity and infrastructure Security Agency , Federal Bureau of Investigation , SecretService Criminal Investigation Department

https://easytech4all.net/2021/05/09/nownext-countering-ransomware-attacks/

Cyber Essentials by Cybersecurity and Infrastructure Security Agency and Department of Homeland Security.

https://easytech4all.net/cyber-essentials-us-dhs/

Ransomware Attackers Defenders - FBI's perspective

https://easytech4all.net/ransomware-attackers-defenders-fbis-perspective/

US Cyberspace Solarium Commission

https://easytech4all.net/2022/04/10/us-cyberspace-solarium-commission/

UK Cybersecurity Association with Digital Police Center.

https://easytech4all.net/uk-cybersecurity-association-1-day-summit/

Fourth Annual Cybersecurity Summit by Cybersecurity and Infrastructure Security Agency .

https://easytech4all.net/2022/02/07/4th-annual-national-cybersecurity-summit-by-cisa/

Fourth CEO Summit - USA

https://easytech4all.net/2022/06/27/iv-ceo-summit-of-the-americas/

State of American Business 2023

https://easytech4all.net/state-of-american-business-2023/?utm_source=pocket_mylist

Challenges faced by Government and international LAW Enforcement

https://easytech4all.net/2021/10/06/watch-challenges-faced-by-govt-and-int-law-enforcement-cybersec-on-youtube/

Intelligence and National Security Alliance (INSA) 2022 UPDATE

https://easytech4all.net/future-of-intelligence-community-workforce/

What is Advanced Cyber Threat Intelligence ?

https://easytech4all.net/2020/09/20/what-is-advanced-cyber-threat-intelligence/

Accreditations Webinars LMS - Cybersec CTI

https://easytech4all.net/2020/12/29/cybersec-accreditation-nanocertifications/

Google Cloud Security Summit with Chris Inglis (National Cyber Director , Executive office of the US President)

https://1powercyber.substack.com/p/google-cloud-security-summit-with

Security information and event management (SIEM) is a field within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware. Vendors sell SIEM as software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes. The term and the initialism SIEM was coined by Mark Nicolett and Amrit Williams of Gartner in 2005.

https://1powercyber.substack.com/p/security-information-and-event-management?utm_source=pocket_mylist

Zero Trust Architectured Networks by Cybersecurity and Infrastructure Security Agency

https://easytech4all.net/2021/10/10/zero-trust-architectured-networks-advanced-cyber-threat-intelligence/

1PowerCyber and Easytech4all Global CTI Research & Analysis.

https://easytech4all.net/internet-ranking-advanced-cyber-threat-intelligence/

https://easytech4all.net/2021/02/21/easytech4all-ranking-for-advanced-cyber-threat-intelligence/

https://easytech4all.net/2020/12/30/3452-best-cybersecurity-stories-by-easytech4all-on-flipboard-quick-updates/

Mapping Global CTI Landscape and Visual Trends

https://easytech4all.net/2021/02/14/mapping-global-ranking-for-advanced-cyber-threat-intelligence/

International Cyber Threat Intelligence Brainstorms

https://easytech4all.net/1-power-cybersec-cti-brainstorms/

Safe and Secure Digital Ecosystem for Schools by US Department of Homeland Security and Department of Justice

https://easytech4all.net/2022/04/10/safe-and-secure-digital-ecosystems-for-students/

Global Cyber Threat Landscape

https://easytech4all.net/cyber-threat-intelligence-landscape/

https://easytech4all.net/cyberwar-ww3-flashpoint/

CyberKinetic and 5G

https://1powercyber.blogspot.com/2022/05/cyber-kinetic-world-war-3-and-5g-in.html?utm_source=pocket_mylist

https://1powercyber.substack.com/p/cyber-kinetic-warfare?utm_source=pocket_mylist

Cyber Independence and Freedom

https://easytech4all.net/2021/08/14/cyber-independence-freedom/

Cyberattacks and Critical Infrastructure (Reading & Resources)

https://easytech4all.net/2021/10/01/cyberattacks-critical-infrastructure-nato/

Space Threats and Satellite Navigation Systems

https://easytech4all.net/2022/03/06/threats-to-satellite-navigation-system-conflict-in-space/

https://1powercyber.substack.com/p/space-threats-satellite-navigation?utm_source=pocket_mylist

Comsec Protocols and Paradigms

https://1powercyber.substack.com/p/comsec-protocols-and-paradigms?utm_source=pocket_mylist

Advanced Cyber Threat Intelligence Landscape and Updates via Digital Magazine by 1PowerCyber for Easytech4all.net

https://bit.ly/3P8gCTT

Advanced Cyber Threat Intelligence Research Analysis Assessment and Projections . Video Playlist .

https://bit.ly/3yqDEje

Advanced Cyber Defense Threat Intelligence Blog in Progress

https://easytech4all.net/author/easytechonline/

https://1powercyber.substack.com

https://1powercyber.blogspot.com

https://easytech4all.tumblr.com/

https://medium.com/@1PowerCyber

References

Clarke R.A, K. R. (2010). Cyber war: the next threat to national. eCCO.

Clarke, R. (2011). Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins.

Cybersecurity and Infrastructure Agency. (2021, October 15). CISA HOME. Retrieved October 14, 2021, from https://www.cisa.gov/about-cisa

Gazula, M. B. (2017). Cyber Warfare Conflict Analysis and Case Studies. Massachusetts Institute of Technology .

Jeremy Rabkin, A. R. (2016). Hacking Back Without Cracking Up. Aegis Paper Series No. 1606.

Kukuh Ugie Sembodho, A. T. (2021). The Limitation of United States Deterrence Strategy Towards North Korean Cyber . Global Strategis, p. 150.

Libicki, M. (2009). Cyberdeterrence and cyberwar. Santa Monica: The Rand Corporation.

M, T. (2012). An analysis for a just cyber warfare in Cyber Conflict (CY-CON). , 2012 4th International Conference on,, (pp. 1-10).

National Security Agency. (2021, October

14). NSA Home.

Parks R, D. D. (2011). Principles of cyberwarfare, security privacy. IEEE, 30-35.

Rid, T. (2012, March). Think Again: Cyberwar. Foreign Policy , pp. 80-84.

Sanger, D. (n.d.). The Perfect Weapon: War, Sabatoge, and Fear in the Cyber Age. New York: Crown Publishers.

Schmitt, M. (2014). The Law of Cyber Warfare: Quo Vadis? Stanford Law & Policy Review, 269-270.

Tallin Mannual. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

The White House. (2011, April). National Strategy for Trusted Identities in

Cyberspace.

The White House. (2021). Improving the Nation’s Cyber

security. Federal Register Vol. 86.

Trautman, L. J. (2016, April). Cybersecurity: What About US Policy? Journal of Law, Technology & Policy, p. 344.

US Cyber Command. (2021). US Cyber Command Mission. Retrieved from https://www.cybercom.mil/About/Mission-and-Vision/

How the threat landscape has changed over time with the advent of AI

AI impact on cybersecurity -

AI Cyberdefense systems are being implemented to proactively detect and

mitigate threats. Traditional antivirus relies on blacklisting historic threats based

on virus signatures. AI based EDR can recognise aspects of software that may be malicious without the need to rely on pre defined database.

MAJOR APPLICATION IN -

EDR - USER AUYHENTICATION - NETWORK DETECTION - INTRUSION DETECTION AND PREVENTION (IDS) - LOG MANAGEMENT AND SIEM.

Behavioural Biometrics identifies users based on unique aspects of their digital activity - Active authentication systems enhance cybersecurity by ensuring ongoing user authentication

CYBER AI 4 ZERO TRUST NETWORK ACCESS (ZTNA) - Intelligent dynamic multi dimensional security approach.

Smart Automation for the complete process. Real time monitoring 2 identify breaches (Alarm React Respond). Intelligent Behavioural Analytics to identify patterns - Erratic Actions through combination of user data + location + user behaviour = Log info 4 future access reference retrieval. If APT breach identified mechanically protect the centralised data vault.

Behavioural Analytics .

Application of complex algorithms to individual level data to derive insights , generate forecasts and make predictions about future human behaviour. Global INTEL Agencies could hypothetically implement AI to make predictions about future behaviour. Major Application - Insider Threat Detection (ITD) - Govt & Military etc.

BA is here to stay. BA techniques may not just be effective in refining assessment of risk but also discovering new leads about evolving cyber threats landscape. Increasingly sophisticated use of AI and BA can be deployed to extract information from bulk datasets.

US Pentagon believes that precognitive AI can predict events 'days in advance' - Global Information Dominance Experiments (GIDE) - AI + CLOUD COMPUTING + SENSORS. Mix of military and civilian sensors to address scenarios where contested logistics might pose a problem. GIDE tech employs ML based system to send fast critical updates and alerts. Can prevent surprise aggression or lead to negotiations instead of conflict . Humans will still be heavily involved in the process.

Complex weapons platforms also coordinate attack or defense among geographically disparate forces. A CyberAttack on these

weapons platforms can crash the software
used to runthem. That could sideline a
fighter jet or radar that protects a aircraft
carrier battlegroup or cause a Military
satellite to go offline using non kinetic
means . Satellite navigation systems are also
at risk of jamming and spoofing. Satellites
are also crucial for coordinating electricity
grids and time stamping financial
transactions. Geolocation is susceptible to
electronic interference.
Penetrating communication networks , sabotaging databases
(deleting spare engines for fighter jets from spare parts roster)
and locking legitimate users out from crucial networks. The NSA
wants military industrial complex to take cyber vulnerabilities
seriously. Unlike the kinetic battlefield where aircraft drones and
armored fighting vehicles spend most of their time out of
contact with the enemy - The wireless nature of computer
networks means that those same weapons will be under constant
threat of enemy assault . And that requires a different kind of
armor.
credit - NATIONAL SECURITY AGENCY.
A Supply chain attack is an incredibly expensive operation . Back doors imitate
legimitate email users and fool the electronic systems that are supposed to assure
identities of users with the right login credentials and additional authentication.
Such an attack has the opportunity to hit a massive quantity of targets but if
reached to far the APT would lose their incredible access - FireEye
Complex Weapon systems and platforms are
vulnerable to Cyber Attack - Weapon Systems don't
just include hypersonic missiles or lasers. There are
computers at wings , at sea and on land. We don't
think of weapons systems that way but none of them
works without computers.These computers add
functionality , including fire control (correcting and
adjusting aim against distant or fast moving
targets), navigation,(receiving AGPS signals) and
communications (voice and data)
UN Appointed independent rights experts - AI Powered spyware &

disinformation is on the rise & regulation of Space has become

urgent.AI based biometric surveillance systems are increasingly being

used in sensitive contexts without individuals knowledge or consent.

Urgent & strict regulatory red lines are needed for technologies that

claim to perform emotion or gender recognition. The Human Rights

Council appointed experts condemned the already alarming use and

impacts of spyware and surveillance technologies on the work of

human rights defenders and journalists often under the guise of

National security and counter terrorism measures

Human Rights Council also called for regulation to address the

lightning fast development of generative AI that's enabling mass

production of fake online content which spreads disinformation

and hate speech. Encryption and Privacy are paramount. They

underlined the need to ensure technical solutions - including

strong end to end encryption and unfettered access to VPNs -

and secure and protect digital communications.

"Adversarial AI" - A Threat to military systems - Shift5's

Lospinoso says - The former Army Captain told a Senate Armed

Services panel how AI can impact Military Operations.

AI for cybersecurity and cybersecurity for AI.

AI in cybersecurity presents great opportunities but as with any powerful general purpose dual use technology , it also brings great challenges. AI can

improve cybersec and defence measures allowing for greater system robustness , resilience and responsiveness but AI in the form of ML and deep learning will escalate sophisticated cyberattacks enabling faster and better targeted and more destructive attacks.

The application of AI in cybersecurity also poses security and ethical concerns.

Among other things it remains unclear to see how responsibilities for autonomous response systems should be ascribed. How to make sure systems

are behaving according to expectations. Or what the security risks carried by the increasing anthropomorphisation of AI systems are.
ANTHROPOMORPHIC LANGUAGE AT TIMES APPEARS INTRINSIC TO THE FIELD OF AL RESEARCH

The Organisation for economic cooperation and development (OECD) defines an AI system as

a “machine based system that can for a given set of human defined objectives make predictions recommendations or decisions influencing real or virtual environments.” This definition has also been accepted and adopted by the European Commission in the Regulation on a European approach for AI.

ML is a set of techniques to allow machines to learn in an automated manner through patterns and inferences rather than through explicit instructions through a human. ML approaches often teach machines to reach an outcome by showing them many examples of correct outcomes. However they can also define a set of rules and let the machine learn by trail and error.

Neural networks involve repeatedly interconnecting thousands or millions of simple transformations into a larger statistical machine that can learn sophisticated relationships between inputs and outputs. Neural networks modify there own code to find and optimise

links between inputs and outputs .

Deep learning is a large neural network subset composed of hierarchical layers that increase

the complexity of the relationships between input and output.

AI in cybersecurity can be identified in 3 categories. - Detection 51% Prediction 34% and response 18%.

Driving forces that are boosting the use of AI in cybersecurity.

1. Speed of impact – in some of the major attacks the average time of impact on the organisation is 4 mins.

Todays attacks are not just ransomware or just targeting certain systems or vulnerabilities they can move and adjust based on what the targets are doing. These kind of attacks impact incredibly quickly and there are not many human interactions that can happen in the meantime.

2. Operational complexity. - Today the proliferation of cloud computing platforms and the fact that those

platforms can be operationalised and deliver services quickly in the milliseconds range. Means that you

cannot have a lot of humans in that loop and you have to think about a more analytics driven capability.

3. Skills gap – There is a global shortage of about a million and a half cybersecurity professionals. This level of scarcity pushes the industry to automate at a faster rate.

AI can help security teams in 3 ways. - By improving systems robustness response and resilience ...The 3R

model.

AI can improve systems robustness that is the ability of a system to maintain its initial assumed stable configuration even when it processes erroneous inputs. Thanks to self testing and self healing software. This means that AI systems can be used to improve testing for robustness delegating to the machines the process of verification and validation.

AI can strengthen systems resilience – the ability of a system to resist and tolerate an attack by facilitating threat and anomaly detection.

AI can be used to enhance response – the capacity of a system to respond autonomously to attacks , to identify vulnerabilities in other machines and to operate strategically by deciding which vulnerability to attack and to launch more aggressive counterattacks.

Identifying when to delegate decision making and response actions to AI and the need of an

individual org to perform risk impact assessment are related. In many cases AI will augment

without replacing the decision making of human security analysts and will be integrated into

the process that accelerate response times.

AI Cyberdefense systems are being implemented to proactively detect and mitigate threats. Traditional antivirus relies on blacklisting historic threats based on virus signatures. AI based EDR can recognise aspects of software that may be malicious without the need to rely on pre defined database.

MAJOR APPLICATION IN -

EDR - USER AUYHENTICATION - NETWORK DETECTION - INTRUSION

DETECTION AND PREVENTION (IDS) - LOG MANAGEMENT AND SIEM.

Behavioural Biometrics identifies users based on unique aspects of their digital activity - Active authentication systems enhance cybersecurity by ensuring ongoing user authentication

CYBER AI 4 ZERO TRUST NETWORK ACCESS (ZTNA) - Intelligent dynamic multi dimensional security approach.

Smart Automation for the complete process. Real time monitoring 2 identify breaches (Alarm React Respond). Intelligent Behavioural Analytics to identify

patterns - Erratic Actions through combination of user data + location + user behaviour = Log info 4 future access reference retrieval. If APT breach identified mechanically protect the centralised data vault.

Behavioural Analytics .

Application of complex algorithms to individual level data to derive insights , generate forecasts and make predictions about future human

behaviour. Global INTEL Agencies could hypothetically implement AI to make predictions about future behaviour. Major Application - Insider

Threat Detection (ITD) - Govt & Military etc.

BA is here to stay. BA techniques may not just be effective in refining assessment of risk but also discovering new leads about evolving cyber

threats landscape. Increasingly sophisticated use of AI and BA can be deployed to extract information from bulk datasets.

US Pentagon believes that precognitive AI can predict events 'days in advance' - Global Information Dominance Experiments (GIDE) - AI + CLOUD COMPUTING + SENSORS. Mix of military and civilian sensors to address scenarios where contested logistics might pose a problem. GIDE tech employs ML based system to send fast critical updates and alerts. Can prevent surprise aggression or lead to negotiations instead of conflict . Humans will still be heavily involved in the process.

Complex weapons platforms also coordinate attack or defense among geographically disparate forces. A CyberAttack on these weapons platforms can crash the software used to runthem. That could sideline a fighter jet or radar that protects a aircraft carrier battlegroup or cause a Military satellite to go offline using non kinetic means - Lasers , radio frequency jammers and Cyberattacks . Satellite navigation systems are also at risk of jamming and spoofing. Satellites are also crucial for coordinating electricity grids and time stamping financial transactions. Geolocation is susceptible to electronic interference.

Penetrating communication networks , sabotaging databases (deleting spare engines for fighter jets from spare parts roster) and locking legitimate users out from crucial networks. The NSA wants military industrial complex to take cyber vulnerabilities seriously. Unlike the kinetic battlefield where aircraft drones and armored fighting vehicles spend most of their time out of contact with the enemy - The wireless nature of computer networks means that those same weapons will be under constant threat of enemy assault . And that requires a different kind of armor.

credit - NATIONAL SECURITY AGENCY.

A Supply chain attack is an incredibly expensive operation . Back doors imitate legimitate email users and fool the electronic systems that are supposed to assure identities of users with the right login credentials and additional authentication.

Such an attack has the opportunity to hit a massive quantity of targets but if reached to far the APT would lose their incredible access - FireEye

Complex Weapon systems and platforms are vulnerable to Cyber Attack - Weapon Systems don't just include hypersonic missiles or lasers. There are computers at wings , at sea and on land. We don't think of weapons systems that way but none of them

works without computers.These computers add

functionality , including fire control (correcting and

adjusting aim against distant or fast moving

targets), navigation,(receiving AGPS signals) and

communications (voice and data)

UN Appointed independent rights experts - AI Powered spyware & disinformation is on the rise & regulation of Space has become urgent.AI based biometric surveillance systems are increasingly being

used in sensitive contexts without individuals knowledge or consent.

Urgent & strict regulatory red lines are needed for technologies that claim to perform emotion or gender recognition. The Human Rights Council appointed experts condemned the already alarming use and

impacts of spyware and surveillance technologies on the work of human rights defenders and journalists often under the guise of National security and counter terrorism measures

Human Rights Council also called for regulation to address the lightning fast development of generative AI that's enabling mass production of fake online content which spreads disinformation

and hate speech. Encryption and Privacy are paramount. They underlined the need to ensure technical solutions - including

strong end to end encryption and unfettered access to VPNs - and secure and protect digital communications.

"Adversarial AI" - A Threat to military systems - Shift5's

Lospinoso says - The former Army Captain told a Senate Armed Services panel how AI can impact Military Operations.

Cyber Intelligent Attacks .

1. AI driven Malware - Artificially intelligent malware can infect devices faster than ever before becoming harder to detect targeting more victims and creating more convincing phishing attacks.

2. Vulnerable Applications - Weak application security creates an entry point for APT to infiltrate computer systems. AI can be used to hide malicious code within applications , sometimes programming the attack to execute well after the app has been installed Malicious codes can be present for years before they strike. Data Obfuscation - An image is worth a thousand lines of malware. Malware hidden in images developed by AI can only be detected by AI.

3. Expanded attack surface - Hybrid work and cloud access in personal devices widens the surface are for cyberattacks. AI creates an even more involved that landscape expanding what devices and machines can be used to infiltrate systems.

4. Constant evolution - AI is always evolving. While the benefits include enhanced threat detection. APT are constantly learning from advanced AI tools to develop more advanced attacks and improve their malware. The dawn of Advanced Intelligent Polymorphic cyber attacks is here.

Therefore it's about time to intelligently automate endpoint security , email security , Application security , identity and access management.

Thanks to

1. NORTH ATLANTIC TREATY ORGANISATION.

2. UN APPOINTED INDEPENDENT RIGHTS EXPERTS.

3. INTELLIGENCE AND NATIONAL SECURITY ALLIANCE.

4. NATIONAL SECURITY AGENCY.

5. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

6. INFORMATION SYSTEMS AND SECURITY ASSOCIATION I

NTERNATIONAL.

7. EUROPEAN DEFENCE AGENCY.

8. EUROPEAN PARLIAMENTARY RESEARCH SERVICE.

1PowerCyber @ easytech4all.net

https://1powercyber.substack.com

https://1powercyber.blogspot.com

https://easytech4all.tumblr.com

https://linktr.ee/1powercyber

CyberAI Analysis.

https://easytech4all.net/2023/08/30/advanced-cyber-threat-intelligence-document-presentation/

https://easytech4all.net/2023/08/30/my-qa-sessions-with-google-bard-large-language-model-a-little-organised-readers-discretion-advised/

https://easytech4all.net/2023/08/28/some-interactions-with-openais-chatgpt4-on-ai-and-relevant-domains-readers-discretion-advised/

https://easytech4all.net/2023/08/28/rendezvous-with-googles-bard-beta/

https://easytech4all.net/2023/09/11/7th-annual-defense-news-conference/

https://1powercyber.substack.com/p/advanced-cyber-threat-intelligence

https://1powercyber.substack.com/p/global-cyber-intelligence-research

https://1powercyber.substack.com/p/cyber-threat-intelligence-reflections

Global Cyber Defense Threat Intelligence Observations.

https://easytech4all.net/2023/03/21/quick-global-cyber-threat-intelligence-observations-22-23/

https://1powercyber.substack.com/p/cyberais-impact-on-cybersecurity

https://1powercyber.substack.com/p/the-evolving-cyber-landscape

Global Cyber Intelligence - Consecrated

https://easytech4all.net/2023/06/07/global-cyber-intelligence-consecrated/

CyberAI - Inter Continental Strategic Imperative.

https://1powercyber.blogspot.com/2023/06/ai-for-cybersecurity-and-cybersecurity.html?m=1

NATO - Strategic Competition in Cyberspace

https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html

Google Cloud Security Conference 2023

https://easytech4all.net/2023/06/07/google-cloud-security-2023/

NATO Locked Shields

https://1powercyber.substack.com/p/nato-locked-shields-2022?utm_source=pocket_mylist

UNIDIR Cyber Stability Conference

https://easytech4all.net/2023/04/02/unidir-cyber-stability-conference-2023/

Blog for work in progress updates on R&A

https://easytech4all.net

https://easytech4all.net/author/easytechonline/

White House National Cybersecurity Strategy

https://www.csoonline.com/article/3689911/white-house-releases-an-ambitious-national-cybersecurity-strategy.html

Countering Ransomware with Department of Homeland Security , Cybersecurity and infrastructure Security Agency , Federal Bureau of Investigation , SecretService Criminal Investigation Department

https://easytech4all.net/2021/05/09/nownext-countering-ransomware-attacks/

Cyber Essentials by Cybersecurity and Infrastructure Security Agency and Department of Homeland Security.

https://easytech4all.net/cyber-essentials-us-dhs/

Ransomware Attackers Defenders - FBI's perspective

https://easytech4all.net/ransomware-attackers-defenders-fbis-perspective/

US Cyberspace Solarium Commission

https://easytech4all.net/2022/04/10/us-cyberspace-solarium-commission/

UK Cybersecurity Association with Digital Police Center.

https://easytech4all.net/uk-cybersecurity-association-1-day-summit/

Fourth Annual Cybersecurity Summit by Cybersecurity and Infrastructure Security Agency .

https://easytech4all.net/2022/02/07/4th-annual-national-cybersecurity-summit-by-cisa/

Challenges faced by Government and international LAW Enforcement

https://easytech4all.net/2021/10/06/watch-challenges-faced-by-govt-and-int-law-enforcement-cybersec-on-youtube/

Intelligence and National Security Alliance (INSA) 2022 UPDATE

https://easytech4all.net/future-of-intelligence-community-workforce/

What is Advanced Cyber Threat Intelligence ?

https://easytech4all.net/2020/09/20/what-is-advanced-cyber-threat-intelligence/

Google Cloud Security Summit with Chris Inglis (National Cyber Director , Executive office of the US President)

https://1powercyber.substack.com/p/google-cloud-security-summit-with

CyberKinetic and 5G

https://1powercyber.blogspot.com/2022/05/cyber-kinetic-world-war-3-and-5g-in.html?utm_source=pocket_mylist

Cyberattacks and Critical Infrastructure (Reading & Resources)

https://easytech4all.net/2021/10/01/cyberattacks-critical-infrastructure-nato/

Space Threats and Satellite Navigation Systems

https://easytech4all.net/2022/03/06/threats-to-satellite-navigation-system-conflict-in-space/

https://1powercyber.substack.com/p/space-threats-satellite-navigation?utm_source=pocket_mylist

Comsec Protocols and Paradigms

https://1powercyber.substack.com/p/comsec-protocols-and-paradigms?utm_source=pocket_mylist

Mapping Global CTI Landscape and Visual Trends

https://easytech4all.net/2021/02/14/mapping-global-ranking-for-advanced-cyber-threat-intelligence/

International Cyber Threat Intelligence Brainstorms

https://easytech4all.net/1-power-cybersec-cti-brainstorms/

Safe and Secure Digital Ecosystem for Schools by US Department of Homeland Security and Department of Justice

https://easytech4all.net/2022/04/10/safe-and-secure-digital-ecosystems-for-students/

Advanced Cyber Threat Intelligence Landscape and Updates via Digital Magazine by 1PowerCyber for Easytech4all.net

https://bit.ly/3P8gCTT

1️⃣ CyberAI and its impact ?

What types of AI are poised for the most growth in 2021 , 2022 and 2023 ?

Why are self-service and predictive analytics growing so much?

How are companies using AI, and specifically virtual assistants, functionally?

Which AI platforms and analytics tools are companies using the most?

What kind of success metrics are they seeing, in areas such as revenue increase, cost decrease, and customer ratings?

2️⃣ Cybersec in Fintech

Despite pouring billions of dollars into security, financial institutions continue to be the number one target of cybercriminals.

The digital transformation undertaken by this industry is contributing to this challenge as it has opened new doors for attackers, making customer data management and protection increasingly difficult.

The huge amount of financial transactions generated by retail organisations poses an attractive target for threat adversaries. While the predominant threat to the retail industry has traditionally been from criminal adversaries leveraging malware designed to compromise Point-of-Sale (PoS) terminals, there has been a marked increase in major ransomware attacks affecting retailers.

3️⃣ Cyber Threat Intelligenc -Brief Analysis

True threat intelligence involves collaboration with peers in industry, cross industry, with law enforcement and with regulatory bodies. It is understood that to call it “intelligence,” TI has to be a public/private community effort. TI also has to be a human/machine community effort.

Fundamentally, organizations must be able to leverage their cyber security to protect everything. From firewalls and devices (whether at the edge or on-site), to data stored in the cloud and the configurations done to process it, policy management is ultimately the glue bonding this together.

Cyber security of the average global corporate enterprise has exponentially improved in recent years. In recent months unprecedented disruption along with unique and innovative threats have been unleashed. As identity has become the new perimeter, organizations have an acute need to further mature Identity & Access Management now.

Threat Intel reports are constantly being released which document the novel techniques and custom tooling that support real world operations. However, despite access to this information, the industry still lacks many of the fundamentals required to emulate nation state threats, opting instead for “off the shelf” tooling and click-once solutions.

Many Security and IT professionals continue to face the challenge of allowing access to employees while ensuring proactive security measures are in place.

The front lines of real-world attacks move faster than defenses can keep up. Public exploits, proof of concepts, defensive bypasses, attack methodologies, and “tricks of the trade” are readily available. To match, sophisticated adversaries are constantly building custom code, integrating public research, and researching 0-day techniques for their operations.

The evolution of the ability to think, operate, and develop tools just like sophisticated, real-world attackers is being observed. This includes the research of defensive bypasses, implementation of public research, and modification of toolkits to accomplish operational goals.

Many Malware Dev initiatives focus on the goals, challenges, architecture, and operations of advanced persistent threat (APT) tooling. Such initiatives dive deep into source code to gain a strong understanding of execution vectors, payload generation, automation, staging, command and control, and exfiltration. They also provide hands-on experience with black hat techniques currently used by hackers to bypass NIDS and HIPS systems, layer 7 web proxies, “next-gen” antivirus, and DLP solutions.

4️⃣ IT security management is critical for operational success — regardless of industry, market or vertical.

For managed security service providers (MSSPs), these expanding attack surfaces and evolving threat vectors represent significant opportunity: If they can provide agile, adaptive security provisioning to manage cloud, big data and mobile needs on-demand, they can capture consumer interest and boost customer conversion.

Threat actors continue to find new ways to use the technologies most integral to businesses – mobile devices, computers, servers, websites, wifi, and email – as entry points to breach networks for malicious purposes.

Remediation-based, orchestrated, automated and customized threat intelligence must be the goal. Most organizations have a few steps to go before reaching that goal. Cyber Security executives have realized that raw data is not intelligence. The discipline is not called Threat Raw Data, it’s called Threat Intelligence. Global corporate enterprise cyber security executives must move past a collective present ‘feed-based’ mindset. To ensure the cyber security community achieves this end-goal

Like APT groups, sophisticated cybercriminals gather as much information about their target before executing the actual attack. Key strategies need to be evolved to implement inorder to protect the SOC team members from social engineering attacks.

No one is immune to cyberattacks; organizations of all types and sizes continue to fall victim to cyberattacks despite all installed security solutions. The new threat landscape has forced organizations to invest in cyber defense, and having a SOC capability has become an essential countermeasure to respond to current and emerging threats.

Social engineering (SE) attacks, especially phishing email, remain the top threat that faces organizations. According to data, 95% of all attacks targeting enterprise networks are caused by spear phishing, and 30% of phishing emails are opened by targeted users, while 12% of these users click on a malicious URL within the email body. Suppose adversaries succeeded in convincing a key SOC member

to give enterprise credentials through social engineering tricks. In that case, a security hole can open in the target organization's defense wall, leading to penetrating its security solutions and possibly leading to a data breach.

Cyber adversaries are exploiting acute vulnerabilities accelerating attacks and introducing increasingly damaging tactics, techniques and procedures. Recently heard about Agnostic Cyber Threat Intelligence - Understanding the totality of your Threat Intel feeds.

As data becomes ever more important for decision making and battlefield control, securing and protecting it is a top priority for the Department of Defense. Technologically advanced competitors are pushing the limits of data security, forcing new strategies, tactics and technology to ensure data can be trusted to be accurate, unadulterated and protected from manipulation or deletion.

The U.S. Department of Defense (DoD) offers one potential profit pathway — according to MxD, the DoD is now spending more than $300 billion each year on contracts. There's a caveat, however: DoD directive 8140 (formerly DoDD 8570) requires that any contractor satisfy specific training and certification provisions to ensure sensitive data remains secure.

The result? There's opportunity for MSSPs under the umbrella of DoD — so long as staff have the right qualifications.

5️⃣ The Red Teamers

Red teaming, the practice of simulating a real-time cyber security attack, is often shrouded in secrecy and allure. While the secrecy and allure may have grown beyond the practice in reality, its benefits are very real. Still, red team culture can often be looked at with an air of skepticism and suspicion.

Despite the large investment many companies have made in detective controls, it's still pretty for motivated Red Teams to take over an entire cyber network during a penetration test or red team engagement, and never trigger a single response ticket. Naturally this has generated some concern at the CISO level as to whether or not a real breach would be detected.

Testing the effectiveness of detective and preventative controls can be a challenge. However, the process can be a lot easier if common attack workflows are understood, and broken into manageable pieces.

Different techniques of ethical hackers are often used and the steps needed to reduce cyber risk through penetration testing, like

• Scoping strategies

• Incorporating vulnerability scans

• Post-test remediation measures

6️⃣ High Profile Breaches and Zero Trust Counter Measure.

In our increasingly cloud-first world, the idea of a trusted internal network zone and an untrusted external one is now outdated. The truth is, today's cyberthreats often get past perimeter defenses undetected, so you can no longer trust data traffic no matter where it originates.

That's where Zero Trust architectures come in. Zero Trust approaches are becoming an urgent priority for enterprise and government organizations alike.

Bird's eye view -

The security trends fueling the adoption of Zero Trust architectures.

The critical role that DNS security plays in successful implementations.

The key elements you need to have in place and next steps to move forward.

Recent high-profile breaches have involved privileged user and service account compromises throughout a network, and 80% of breaches involve credentials and identity. The bottom line is that anyone can get hacked and have a persistent privileged user lurking somewhere on their network.

With a Zero Trust solution, you can add security to your identity store without having your users spend minutes every day authenticating into their basic systems — and a frictionless Zero Trust solution can also reduce security complexity, save money, and reduce time to identify and remediate breaches.

80% of breaches involve credentials. Any identity can be compromised to launch large scale, persistent attacks on enterprises. With the increase in digital transformation, enterprises are looking to implement and fine-tune the Zero Trust security strategy to prevent sophisticated cyber-attacks.

With the increase in digital transformation, enterprises are looking to implement and fine-tune the Zero Trust security strategy to prevent sophisticated cyber-attacks.

The importance of having an effective PAM strategy to tackle prominent challenges like insider threats, how to balance security and operational efficiency, and more.

➤ Getting PAM fundamentals like Zero Trust, the principle of least privilege (PoLP), and just-in-time (JIT) security models right.

➤ Today advanced analytics and forensic audits are important for all privileged access.

On the Job 24X7 - 365 days - Cybersecurity managers, architects and professionals tasked with keeping data safe even as their networks become increasingly borderless.

7️⃣ Secure Access Tools and MFA.

Secure access tools can only be effective if the business remains enabled. Users can only be as effective as the access they are granted allows.

Multi factor authentication' of secure access technology should include not only architectural interoperability but interoperability with your human resources.

The Access Brokers play a pivotal role in eCrime ecosystem. Ransomware Actors are rapidly adopting Data Extortion methods. Highly anticipated updates on top cyber threats and adversaries by Global Cyber Intel Think Tank , reveals observed trends in attackers' ever-evolving tactics, techniques and procedures and offers practical recommendations to protect your organization

The Sevens of MFA and ZTNA.

1.Examining everything through a risk management lens.

2.Auditing the end-to-end awareness program and doing more than rolling out the same thing again.

3.Unpacking desired behaviors and heat maps to gain more insight.

4.Expediting different yet active learning with nuanced targeted audiences.

5.Perfecting the art of the nudge.

6.Discovering the relationship between Secure Access technologies and Secure Access mindsets.

7.Realizing that Zero Trust technologies only work with Users' Full Trust of the security operation.

8️⃣ Cloud Security

More companies are using the cloud — as noted by CIO, 96 percent of organizations now use some type of public, private, or hybrid cloud service to help streamline operations and boost IT impact.

As a result, the cloud market is diversifying, with frontrunner Amazon now challenged by up-and-coming cloud providers, including Google, Microsoft, and IBM. Smaller and more specific offerings have also emerged as companies look to tackle top-priority issues, including access management, information security, and big data analysis.

The cloud subjects the enterprise to new and different vulnerabilities. But it also presents the organization with new tools to secure the company via innovative means. And regarding insider threats, the cloud provides multiple layers of insight from which cyber security executives can glean and adapt according.

For IT professionals, this evolving technology landscape means a commensurate uptick in the number and types of cloud certifications available. While virtually all have value in the right circumstance, technology staff making the jump to cloud career tracks are best served by finding the best fit for current and future endeavors.

Cloud security architectural design decisions affect the ability of security vendors to provide a performant, scalable, and reliable platform.

About 48% of contact centers are using cloud platforms, whether multi-tenant CCaaS or single-server hosted and managed. And nearly half of those using cloud contact center say the implementation was better than expected. At the same time, 22% of those who have moved to the cloud say they prefer on-premises—and 7% of those changing architectures by 2022 are moving back to on premises.

Internal reflections on Cloud Network Adoption.

- If you're platform is on-premises, is it time to move to the cloud?

- How can you leverage the cloud without moving the entire platform?

- How does CPaaS fit into the CX architecture decision?

9️⃣ Cybersecurity Automation.

While automation might happen with the click of a button, the quality of the data going in will determine the quality of the data coming out. But that's just the data. The talent needed to work with the data going in and coming out- along with the continual tweaking of the automation tool itself must be in-house. So while one of the promises of automation is to reduce cost, adding automation-focused talent is necessary in order to gain true threat intelligence for the enterprise.

In moving past the feed-based mindset, the context of the evidence-based data being offered must be known. Sharing insights within the community is of paramount importance. The assessment of the insights coming out of that data can become proven organizational knowledge. That knowledge needs to be orchestrated so that action-based response and ultimately remediation can occur.

Cyber Threat Advanced Intelligence platforms like Google Chronicle are transforming petabyte-scale data into visual attack stories: MalOps (malicious operations). With built-in response capabilities and predictive AI, you can achieve 10x the security results without 10x the work. The result: prevent ransomware, find and end attacks across your full environment, and predict where attackers will strike next.

Advanced analytics and machine learning are powering threat intelligence, and enabling threat researchers to:

1.Conduct qualified and detailed threat assessments that can help keep a business secure.

2.Detect malicious anomalies in internet traffic and catch cyber security threats before they seriously impact cyber network.

3.Gaining total visibility of the attack surface and better determining what is needed to do to prevent future cyberattacks

4.Utilisation of the ATT&CK knowledge base in the security strategy.

🔟 DNS over TLS (DoT) and DNS over HTTPS (DoH)

Cyber attackers love targeting the Domain Name System (DNS) because of its pervasive nature and because security teams often overlook DNS as a line of defence.

Overlooking DNS as part of your organisation’s security posture is a mistake.

DOT and DOH have become increasingly newsworthy as some leading technology companies, including computer software and web browser developers, are now enabling these new protocols by default. Historically, communications between DNS clients and servers rarely are encrypted, leaving users vulnerable to spoofing, interception, and other attack types.

DoT and DoH were created to solve these issues, but there's a catch. While DoT and DoH help improve DNS privacy, they can also cause significant changes to how browsers, applications and some operating systems function. This allows users to sidestep your traditional DNS controls – increasing exposure to risks and hampering enterprise visibility. Even worse: it's probably happening on your network. Right now.

1️⃣1️⃣ Advanced enterprise approach by the security operation

It can be expedited by a Business Information Security Officer. And through expediting an advanced enterprise approach, that BISO can turn security into a bottom-line contributing operation. Aligning Privacy and IT Risk to Combat Cyber Threats is happening globally. Identify technology and processing methods to update data in real-time to categorize data elements across risk and control inventories for multi-dimensional risk reporting; Privacy-focused data minimization can help you decrease your overall attack surface; Engage your line of business stakeholders to guide and collaborate with risk managers to remediate risk at the source.

1️⃣2️⃣ Achieving Cyber Resilience - Connecting Dots beyond Cybersecurity.

Cyber security of the average global corporate enterprise has exponentially improved in recent years. In recent times unprecedented disruption along with unique and innovative threats have been unleashed. As identity has become the new perimeter, organizations have an acute need to further mature Identity & Access Management now.

When it comes to operational security, a holistic risk-based approach allows teams to break down every level of the business to provide first-class security for the organisation.

The evolution of essential, core pillars of an effective approach to security - Telemetry Science consolidated through XDR and SIEM. Analysts say XDR and SIEM are on a collision course. The cloud-native CTI platforms today enables a proactive, complete detection and response program. You’ll own your entire attack surface. Experience less noise, more signal with embedded threat intelligence, and automated response.

1️⃣3️⃣ Fortify your DSS

SQL stands for Structured Query Language and is used to store, manipulate, and retrieve databases. The SQL language can perform actions such as executing queries, retrieving data, inserting and deleting records, and so much more. Database system software such as MySQL, SQL Server, MS Access, Oracle, Sybase, Informix, and Postgres utilize SQL to store data for web sites. If an attacker can exploit a web sites SQL database, they will gain a plethora of information. This information can range from email addresses and phone numbers to passwords and social security numbers.

Now that we know what SQL is, what is SQL Injection? A SQL Injection (SQLI) is a vulnerability that gives an attacker the ability to view or alter data they couldn't typically interact with.

Quick Look up -

data exfiltration and infiltration

• malware infiltration

• malware detection

• ecosystem integrations for streamlining operations

• Cyberthreat investigation and intelligence.

1️⃣4️⃣ Phishing is the number one type of cyber crime that remains a continuous threat because cybercriminals are always changing their phishing tactics.

Getting a phishing email does not mean you have to fall for it. There are ways to protect your workplace from phishing.

Managing Phishing through automated cyber counter measures -

1.Monitors top human attack vectors (Phishing, Passwords, Sensitive data handling, Physical security, Flexible working, Devices handling)

2.Identifyvulnerable departments and roles.

3.Provides actionable insights to identify vulnerabilities and inform strategy.

What makes such solutions unique?

Employees are assessed in a friendly and interactive environment that doesn't set them up for failure (unlike phishing simulations). Instant feedback provides guidance and a chance to learn.

1️⃣5️⃣ Cybersecurity Industry and Critical Shortage of Skilled Professionals.

The cybersecurity industry is facing a critical shortage of skilled professionals, with a global demand for 3.4 million experts far exceeding the available supply. This shortage poses significant risks to organizations, as 60 percent of businesses are vulnerable to cyber breaches due to the lack of cybersecurity talent, and 74 percent of breaches involve a human element. Misconfigured systems, slow patches, poor risk assessment, and rushed deployments also contribute to the challenges. Additionally, high turnover rates and burnout among cybersecurity professionals impact long-term security strategies. Despite these challenges, emerging technologies such as generative artificial intelligence, quantum computing, automation, and blockchain offer potential solutions to support the strained cybersecurity workforce.

@NATO @nato.military @NATONews @usarmy @DeptofDefense @INSAEvents @ISSAIntl @NationalSecurityAgencyGov @unitednations

Social Engineering Deepfakes & Disinformation Countermeasures

Highlighted the dangers of Dis/Mis information and Deepfakes around 2 years back. The Blogpost includes resources from US Department of Defense , NATO and German Government – offset AI Powered Disinfo deepfakes and Augment AI as an effective credible Countermeasure to deter future incidents in its tracks.

Deepfake Threats and Countermeasures

Artificial intelligence (AI) can play a crucial role in combating the spread and impact of deepfakes by employing various techniques to detect, prevent, and mitigate the harm caused by these manipulated media. Here are some specific ways in which AI can serve as a countermeasure against deepfakes:

1. Deepfake Detection:

AI-powered deepfake detection tools can analyze audio, video, and text content to identify subtle anomalies and patterns that are indicative of manipulation. These tools employ machine learning algorithms trained on large datasets of real and fake media to learn the telltale signs of deepfakes, such as inconsistencies in facial expressions, skin texture, lighting, and audio synchronization.

2. Content Authentication:

AI-based content authentication techniques can embed digital fingerprints or watermarks into media content, creating a unique identifier that can be used to verify the authenticity of the content. These watermarks are designed to be resilient to manipulation and can be detected even if the content has been altered.

3. Media Provenance Verification:

AI algorithms can analyze the metadata and history of media content to track its origins and identify potential sources of manipulation. This can help to establish the authenticity of content and identify potential deepfakes that have been circulating online.

4. Social Media Monitoring:

AI-powered social media monitoring tools can scan social media platforms for potentially harmful deepfakes, identifying and flagging content that is likely to spread misinformation or cause harm. This can help to limit the reach of deepfakes and prevent them from causing widespread damage.

5. Public Awareness Campaigns:

AI-based tools can be used to create personalized and targeted public awareness campaigns that educate people about deepfakes and how to identify them. These campaigns can help to reduce the susceptibility of individuals to deepfake manipulation and promote critical thinking in the digital age.

In addition to these specific applications, AI can also contribute to the development of more sophisticated deepfake detection and prevention methods. As AI research continues to advance, we can expect to see even more innovative and effective ways to combat deepfakes and protect against their harmful effects.

Here's a list of some open-source (FOSS) tools to detect deepfakes:

Deepstar: Developed by ZeroFox, Deepstar is an open-source toolkit that provides a suite of tools for detecting, analyzing, and mitigating deepfakes. It includes a curated library of deepfake and real videos, a plug-in framework for testing and comparing different detection algorithms, and code for aiding in the creation of deepfake datasets.

FakeFinder: Created by IQT Labs, FakeFinder is an open-source framework that utilizes a combination of deep learning models and traditional image processing techniques to detect deepfakes. It aims to provide a comprehensive and robust solution for identifying manipulated media.

DeepSafe: Developed by Siddharth Sah, DeepSafe is an open-source deepfake detection platform that aggregates various detection models and provides a dashboard for visualizing and analyzing results. It also facilitates the creation of a dataset of potentially harmful deepfakes for further research and improvement of detection methods.

Visual DeepFake Detection: This open-source tool takes a different approach to deepfake detection, focusing on identifying anomalies in facial expressions, eye movements, and skin texture. It utilizes a combination of traditional image analysis techniques and machine learning to detect subtle signs of manipulation.

FALdetector: This open-source tool in Python is designed to detect Photoshopped faces by analyzing image metadata and identifying inconsistencies in lighting, shadows, and color patterns. It primarily focuses on detecting manipulations in still images rather than videos.

Deepware Scanner: Developed by Deepware, Deepware Scanner is an open-source forensic tool that analyzes videos for signs of deepfaking. It employs a deep learning model trained on a large dataset of real and fake videos to identify anomalies and inconsistencies.

Reality Defender: Developed by Sensity, Reality Defender is an open-source deepfake detection tool that utilizes a combination of machine learning and image processing techniques to identify manipulated media. It is designed to be easily integrated into existing applications and workflows.

DFV: Developed by the University of California, Berkeley, DFV is an open-source deepfake detection framework that utilizes a combination of spatial and temporal features to identify manipulated videos. It is designed to be lightweight and efficient, making it suitable for real-time applications.

DeepFake-o-Meter: This open-source tool provides a web-based interface for detecting deepfakes. It utilizes a combination of machine learning algorithms to analyze videos and provide a probability score indicating the likelihood of manipulation.

Open Video Prediction Model (OVPM): Developed by Facebook AI Research, OVPM is an open-source deep learning model for detecting deepfakes. It is trained on a large dataset of real and fake videos and can be used to identify manipulated videos with high accuracy.

These open-source tools represent a growing effort to combat the spread of deepfakes and protect against their harmful effects. As research continues to advance, we can expect to see even more sophisticated and effective FOSS tools emerge in the future.

https://www.linkedin.com/posts/danish-khan-easytech4all_deepfake-media-artificialintelligence-activity-6771673460205776896-1doe

NATO's Approach to Countering Disinformation

https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en

US Department of Defense Approach – Deepfake Disinfo Countermeasures

https://drive.google.com/file/d/1Jpd1yXGk12jixN7Fln-kc0ewOhbgl0KW/view?usp=drivesdk

German Government's approach to countering disinformation and Deepfakes

https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Misc Resources

https://www.scirp.org/journal/paperinformation.aspx?paperid=112520

https://www.semanticscholar.org/paper/DEEPFAKES%3A-THREATS-AND-COUNTERMEASURES-SYSTEMATIC-Albahar-Almalki/cd1cbbe9b7e5cb47c9f3aaf1b475d4694d9b2492

https://link.springer.com/article/10.1007/s10489-022-03766-z

https://www.socialproofsecurity.com/

Meet Rachel Tobac – Social Engineering and Disinformation Countermeasures.

Download Countersocial

CounterSocial – A Next-Gen Social Network

A unique social network. No trolls. No abuse. No ads. No fake-news. No foreign influence operations.

CounterSocial is the first Social Network Platform to take a zero-tolerance stance to hostile nations, bot accounts, trolls and disinformation networks who are weaponizing OUR own social media platforms and freedoms to engage in influence operations against us.

And we're here to counter it.

CounterSocial is 100% crowd powered by it's users, and does not run ads or 'promoted content'. Our users data is not mined or sold for any purpose.

https://play.google.com/store/apps/details?id=counter.social.android

Cyberspace Origins and Frontier AI

Frontier AI

"ARPANET Maps 1969 to 1977". California State University, Dominguez Hills (CSUDH). 4 January 1978. Archived from the original on 19 April 2012. Retrieved 17 May 2012.

Walden, David C. (February 2003). "Looking back at the ARPANET effort, 34 years later". Living Internet. East Sandwich, Massachusetts. Retrieved 19 March 2021.

"Images of ARPANET from 1964 onwards". The Computer History Museum. Retrieved 29 August 2004. Timeline.

"Paul Baran and the Origins of the Internet". RAND Corporation. Retrieved 3 September 2005.

Kleinrock, Leonard. "The Day the Infant Internet Uttered its First Words". UCLA. Retrieved 11 November 2004. Personal anecdote of the first message ever sent over the ARPANET

"Doug Engelbart's Role in ARPANET History". 2008. Retrieved 3 September 2009.

Waldrop, Mitch (April 2008). "DARPA and the Internet Revolution". 50 years of Bridging the Gap. DARPA. pp. 78–85. Archived from the original on 15 September 2012. Retrieved 26 August 2012.

"Robert X Cringely: A Brief History of the Internet". YouTube. Archived from the original on 20 March 2013.

Blog for work in progress updates on R&A

https://easytech4all.net

https://easytech4all.net/author/easytechonline/

Cybersec YouTube playlist.

https://youtube.com/playlist?list=PLf-aX7Sa0eCRYUADIqTAU2qH-lKcNB-wj

https://1PowerCyber.substack.com

https://1PowerCyber.blogspot.com

https://medium.com/@1PowerCyber

https://easytech4all.tumblr.com

Digital Magazine.

https://flipboard.com/@easytech4all/cybersecurity-6tbejh5oz

https://linktr.ee/1powercyber

https://in.linkedin.com/in/danish-khan-a2b169150

Internet Lookup –

“The UK Bletchley Declaration on AI”
“US President Executive Order – Data and AI Strategy”
“The US Department of Defense AI Adoption Strategy”

https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/

https://www.cisa.gov/ai

https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en

Blog for work in progress updates on R&A

https://easytech4all.net

https://easytech4all.net/author/easytechonline/

Cybersec YouTube playlist.

https://youtube.com/playlist?list=PLf-aX7Sa0eCRYUADIqTAU2qH-lKcNB-wj

https://1PowerCyber.substack.com

https://1PowerCyber.blogspot.com

https://medium.com/@1PowerCyber

https://easytech4all.tumblr.com

Digital Magazine.

https://flipboard.com/@easytech4all/cybersecurity-6tbejh5oz

https://linktr.ee/1powercyber

https://in.linkedin.com/in/danish-khan-a2b169150

Recap of Advanced Cyber Threat Intelligence Paradigms & Countermeasures – NCAM Oct(10) 2023

1️⃣ CyberAI and its impact ?

What types of AI are poised for the most growth in 2021 , 2022 and 2023 ?
Why are self-service and predictive analytics growing so much?
How are companies using AI, and specifically virtual assistants, functionally?
Which AI platforms and analytics tools are companies using the most?
What kind of success metrics are they seeing, in areas such as revenue increase, cost decrease, and customer ratings?

2️⃣ Cybersec in Fintech

Despite pouring billions of dollars into security, financial institutions continue to be the number one target of cybercriminals.

The digital transformation undertaken by this industry is contributing to this challenge as it has opened new doors for attackers, making customer data management and protection increasingly difficult.

The huge amount of financial transactions generated by retail organisations poses an attractive target for threat adversaries. While the predominant threat to the retail industry has traditionally been from criminal adversaries leveraging malware designed to compromise Point-of-Sale (PoS) terminals, there has been a marked increase in major ransomware attacks affecting retailers.

3️⃣ Cyber Threat Intelligenc -Brief Analysis

True threat intelligence involves collaboration with peers in industry, cross industry, with law enforcement and with regulatory bodies. It is understood that to call it “intelligence,” TI has to be a public/private community effort. TI also has to be a human/machine community effort.

Fundamentally, organizations must be able to leverage their cyber security to protect everything. From firewalls and devices (whether at the edge or on-site), to data stored in the cloud and the configurations done to process it, policy management is ultimately the glue bonding this together.

Cyber security of the average global corporate enterprise has exponentially improved in recent years. In recent months unprecedented disruption along with unique and innovative threats have been unleashed. As identity has become the new perimeter, organizations have an acute need to further mature Identity & Access Management now.

Threat Intel reports are constantly being released which document the novel techniques and custom tooling that support real world operations. However, despite access to this information, the industry still lacks many of the fundamentals required to emulate nation state threats, opting instead for “off the shelf” tooling and click-once solutions.

Many Security and IT professionals continue to face the challenge of allowing access to employees while ensuring proactive security measures are in place.

The front lines of real-world attacks move faster than defenses can keep up. Public exploits, proof of concepts, defensive bypasses, attack methodologies, and “tricks of the trade” are readily available. To match, sophisticated adversaries are constantly building custom code, integrating public research, and researching 0-day techniques for their operations.

The evolution of the ability to think, operate, and develop tools just like sophisticated, real-world attackers is being observed. This includes the research of defensive bypasses, implementation of public research, and modification of toolkits to accomplish operational goals.

Many Malware Dev initiatives focus on the goals, challenges, architecture, and operations of advanced persistent threat (APT) tooling. Such initiatives dive deep into source code to gain a strong understanding of execution vectors, payload generation, automation, staging, command and control, and exfiltration. They also provide hands-on experience with black hat techniques currently used by hackers to bypass NIDS and HIPS systems, layer 7 web proxies, “next-gen” antivirus, and DLP solutions.

4️⃣ IT security management is critical for operational success — regardless of industry, market or vertical.

For managed security service providers (MSSPs), these expanding attack surfaces and evolving threat vectors represent significant opportunity: If they can provide agile, adaptive security provisioning to manage cloud, big data and mobile needs on-demand, they can capture consumer interest and boost customer conversion.

Threat actors continue to find new ways to use the technologies most integral to businesses – mobile devices, computers, servers, websites, wifi, and email – as entry points to breach networks for malicious purposes.

Remediation-based, orchestrated, automated and customized threat intelligence must be the goal. Most organizations have a few steps to go before reaching that goal. Cyber Security executives have realized that raw data is not intelligence. The discipline is not called Threat Raw Data, it’s called Threat Intelligence. Global corporate enterprise cyber security executives must move past a collective present ‘feed-based’ mindset. To ensure the cyber security community achieves this end-goal

Like APT groups, sophisticated cybercriminals gather as much information about their target before executing the actual attack. Key strategies need to be evolved to implement inorder to protect the SOC team members from social engineering attacks.

No one is immune to cyberattacks; organizations of all types and sizes continue to fall victim to cyberattacks despite all installed security solutions. The new threat landscape has forced organizations to invest in cyber defense, and having a SOC capability has become an essential countermeasure to respond to current and emerging threats.

Social engineering (SE) attacks, especially phishing email, remain the top threat that faces organizations. According to data, 95% of all attacks targeting enterprise networks are caused by spear phishing, and 30% of phishing emails are opened by targeted users, while 12% of these users click on a malicious URL within the email body. Suppose adversaries succeeded in convincing a key SOC member to give enterprise credentials through social engineering tricks. In that case, a security hole can open in the target organization’s defense wall, leading to penetrating its security solutions and possibly leading to a data breach.

Cyber adversaries are exploiting acute vulnerabilities accelerating attacks and introducing increasingly damaging tactics, techniques and procedures. Recently heard about Agnostic Cyber Threat Intelligence – Understanding the totality of your Threat Intel feeds.

As data becomes ever more important for decision making and battlefield control, securing and protecting it is a top priority for the Department of Defense. Technologically advanced competitors are pushing the limits of data security, forcing new strategies, tactics and technology to ensure data can be trusted to be accurate, unadulterated and protected from manipulation or deletion.

The U.S. Department of Defense (DoD) offers one potential profit pathway — according to MxD, the DoD is now spending more than $300 billion each year on contracts. There’s a caveat, however: DoD directive 8140 (formerly DoDD 8570) requires that any contractor satisfy specific training and certification provisions to ensure sensitive data remains secure.

The result? There’s opportunity for MSSPs under the umbrella of DoD — so long as staff have the right qualifications.

5️⃣ The Red Teamers

Red teaming, the practice of simulating a real-time cyber security attack, is often shrouded in secrecy and allure. While the secrecy and allure may have grown beyond the practice in reality, its benefits are very real. Still, red team culture can often be looked at with an air

of skepticism and suspicion.

Despite the large investment many companies have made in detective controls, it's still pretty for motivated Red Teams to take over an entire cyber network during a penetration test or red team engagement, and never trigger a single response ticket. Naturally this has generated some concern at the CISO level as to whether or not a real breach would be detected.

Testing the effectiveness of detective and preventative controls can be a challenge. However, the process can be a lot easier if common attack workflows are understood, and broken into manageable pieces.

Different techniques of ethical hackers are often used and the steps needed to reduce cyber risk through penetration testing, like

Scoping strategies
Incorporating vulnerability scans
Post-test remediation measures 6️⃣ High Profile Breaches and Zero Trust Counter Measure.
In our increasingly cloud-first world, the idea of a trusted internal network zone and an untrusted external one is now outdated. The truth is, today's cyberthreats often get past perimeter defenses undetected, so you can no longer trust data traffic no matter where it originates.

That's where Zero Trust architectures come in. Zero Trust approaches are becoming an urgent priority for enterprise and government organizations alike.

Bird's eye view –
The security trends fueling the adoption of Zero Trust architectures.
The critical role that DNS security plays in successful implementations.
The key elements you need to have in place and next steps to move forward.

Recent high-profile breaches have involved privileged user and service account compromises throughout a network, and 80% of breaches involve credentials and identity. The bottom line is that anyone can get hacked and have a persistent privileged user lurking somewhere on their network.

With a Zero Trust solution, you can add security to your identity store without having your users spend minutes every day authenticating into their basic systems — and a frictionless Zero Trust solution can also reduce security complexity, save money, and reduce time to identify and remediate breaches.

80% of breaches involve credentials. Any identity can be compromised to launch large scale, persistent attacks on enterprises. With the increase in digital transformation, enterprises are looking to implement and fine-tune the Zero Trust security strategy to prevent sophisticated cyber-attacks.

With the increase in digital transformation, enterprises are looking to implement and fine-tune the Zero Trust security strategy to prevent sophisticated cyber-attacks.

The importance of having an effective PAM strategy to tackle prominent challenges like insider threats, how to balance security and operational efficiency, and more.
➤ Getting PAM fundamentals like Zero Trust, the principle of least privilege (PoLP), and just-in-time (JIT) security models right.
➤ Today advanced analytics and forensic audits are important for all privileged access.

On the Job 24X7 – 365 days – Cybersecurity managers, architects and professionals tasked with keeping data safe even as their networks become increasingly borderless.

7️⃣ Secure Access Tools and MFA.

Secure access tools can only be effective if the business remains enabled. Users can only be as effective as the access they are granted allows.

Multi factor authentication' of secure access technology should include not only architectural interoperability but interoperability with your human resources.

The Access Brokers play a pivotal role in eCrime ecosystem. Ransomware Actors are rapidly adopting Data Extortion methods. Highly anticipated updates on top cyber threats and adversaries by Global Cyber Intel Think Tank , reveals observed trends in attackers' ever-evolving tactics, techniques and procedures and offers practical recommendations to protect your organization

The Sevens of MFA and ZTNA.

1.Examining everything through a risk management lens.
2.Auditing the end-to-end awareness program and doing more than rolling out the same thing again.
3.Unpacking desired behaviors and heat maps to gain more insight.
4.Expediting different yet active learning with nuanced targeted audiences.
5.Perfecting the art of the nudge.
6.Discovering the relationship between Secure Access technologies and Secure Access mindsets.
7.Realizing that Zero Trust technologies only work with Users' Full Trust of the security operation.

8️⃣ Cloud Security

More companies are using the cloud — as noted by CIO, 96 percent of organizations now use some type of public, private, or hybrid cloud service to help streamline operations and boost IT impact.

As a result, the cloud market is diversifying, with frontrunner Amazon now challenged by up-and-coming cloud providers, including Google, Microsoft, and IBM. Smaller and more specific offerings have also emerged as companies look to tackle top-priority issues, including access management, information security, and big data analysis.

The cloud subjects the enterprise to new and different vulnerabilities. But it also presents the organization with new tools to secure the company via innovative means. And regarding insider threats, the cloud provides multiple layers of insight from which cyber security executives can glean and adapt according.

For IT professionals, this evolving technology landscape means a commensurate uptick in the number and types of cloud certifications available. While virtually all have value in the right circumstance, technology staff making the jump to cloud career tracks are best served by finding the best fit for current and future endeavors.

Cloud security architectural design decisions affect the ability of security vendors to provide a performant, scalable, and reliable platform.

About 48% of contact centers are using cloud platforms, whether multi-tenant CCaaS or single-server hosted and managed. And nearly half of those using cloud contact center say the implementation was better than expected. At the same time, 22% of those who have moved to the cloud say they prefer on-premises—and 7% of those changing architectures by 2022 are moving back to on premises.

Internal reflections on Cloud Network Adoption.

If you're platform is on-premises, is it time to move to the cloud?
How can you leverage the cloud without moving the entire platform?
How does CPaaS fit into the CX architecture decision? 9️⃣ Cybersecurity Automation.
While automation might happen with the click of a button, the quality of the data going in will determine the quality of the data coming out. But that's just the data. The talent needed to work with the data going in and coming out- along with the continual tweaking of the automation tool itself must be in-house. So while one of the promises of automation is to reduce cost, adding automation-focused talent is necessary in order to gain true threat intelligence for the enterprise.

In moving past the feed-based mindset, the context of the evidence-based data being offered must be known. Sharing insights within the community is of paramount importance. The assessment of the insights coming out of that data can become proven organizational knowledge. That knowledge needs to be orchestrated so that action-based response and ultimately remediation can occur.

Cyber Threat Advanced Intelligence platforms like Google Chronicle are transforming petabyte-scale data into visual attack stories: MalOps (malicious operations). With built-in response capabilities and predictive AI, you can achieve 10x the security results without 10x the work. The result: prevent ransomware, find and end attacks across your full environment, and predict where attackers will strike next.

Advanced analytics and machine learning are powering threat intelligence, and enabling threat researchers to:

1.Conduct qualified and detailed threat assessments that can help keep a business secure.
2.Detect malicious anomalies in internet traffic and catch cyber security threats before they seriously impact cyber network.
3.Gaining total visibility of the attack surface and better determining what is needed to do to prevent future cyberattacks
4.Utilisation of the ATT&CK knowledge base in the security strategy.

🔟 DNS over TLS (DoT) and DNS over HTTPS (DoH)

Cyber attackers love targeting the Domain Name System (DNS) because of its pervasive nature and because security teams often overlook DNS as a line of defence.

Overlooking DNS as part of your organisation's security posture is a mistake.

DOT and DOH have become increasingly newsworthy as some leading technology companies, including computer software and web browser developers, are now enabling these new protocols by default. Historically, communications between DNS clients and servers rarely are encrypted, leaving users vulnerable to spoofing, interception, and other attack types.

DoT and DoH were created to solve these issues, but there's a catch. While DoT and DoH help improve DNS privacy, they can also cause significant changes to how browsers, applications and some operating systems function. This allows users to sidestep your traditional DNS controls – increasing exposure to risks and hampering enterprise visibility. Even worse: it's probably happening on your network. Right now.

1️⃣1️⃣ Advanced enterprise approach by the security operation

It can be expedited by a Business Information Security Officer. And through expediting an advanced enterprise approach, that BISO can turn security into a bottom-line contributing operation. Aligning Privacy and IT Risk to Combat Cyber Threats is happening globally. Identify technology and processing methods to update data in real-time to categorize data elements across risk and control inventories for multi-dimensional risk reporting; Privacy-focused data minimization can help you decrease your overall attack surface; Engage your line of business stakeholders to guide and collaborate with risk managers to remediate risk at the source.

1️⃣2️⃣ Achieving Cyber Resilience – Connecting Dots beyond Cybersecurity.

Cyber security of the average global corporate enterprise has exponentially improved in recent years. In recent times unprecedented disruption along with unique and innovative threats have been unleashed. As identity has become the new perimeter, organizations have an acute need to further mature Identity & Access Management now.

When it comes to operational security, a holistic risk-based approach allows teams to break down every level of the business to provide first-class security for the organisation.

The evolution of essential, core pillars of an effective approach to security – Telemetry Science consolidated through XDR and SIEM. Analysts say XDR and SIEM are on a collision course. The cloud-native CTI platforms today enables a proactive, complete detection and response program. You'll own your entire attack surface. Experience less noise, more signal with embedded threat intelligence, and automated response.

1️⃣3️⃣ Fortify your DSS

SQL stands for Structured Query Language and is used to store, manipulate, and retrieve databases. The SQL language can perform actions such as executing queries, retrieving data, inserting and deleting records, and so much more. Database system software such as MySQL, SQL Server, MS Access, Oracle, Sybase, Informix, and Postgres utilize SQL to store data for web sites. If an attacker can exploit a web sites SQL database, they will gain a plethora of information. This information can range from email addresses and phone numbers to passwords and social security numbers.

Now that we know what SQL is, what is SQL Injection? A SQL Injection (SQLI) is a vulnerability that gives an attacker the ability to view or alter data they couldn't typically interact with.

Quick Look up –

data exfiltration and infiltration

malware infiltration
malware detection
ecosystem integrations for streamlining operations
Cyberthreat investigation and intelligence.
1️⃣4️⃣ Phishing is the number one type of cyber crime that remains a continuous threat because cybercriminals are always changing their phishing tactics.
Getting a phishing email does not mean you have to fall for it. There are ways to protect your workplace from phishing.

Managing Phishing through automated cyber counter measures –

1.Monitors top human attack vectors (Phishing, Passwords, Sensitive data handling, Physical security, Flexible working, Devices handling)
2.Identifyvulnerable departments and roles.
3.Provides actionable insights to identify vulnerabilities and inform strategy.

What makes such solutions unique?

Employees are assessed in a friendly and interactive environment that doesn't set them up for failure (unlike phishing simulations). Instant feedback provides guidance and a chance to learn.

1️⃣5️⃣ Cybersecurity Industry and Critical Shortage of Skilled Professionals.

The cybersecurity industry is facing a critical shortage of skilled professionals, with a global demand for 3.4 million experts far exceeding the available supply. This shortage poses significant risks to organizations, as 60 percent of businesses are vulnerable to cyber breaches due to the lack of cybersecurity talent, and 74 percent of breaches involve a human element. Misconfigured systems, slow patches, poor risk assessment, and rushed deployments also contribute to the challenges. Additionally, high turnover rates and burnout among cybersecurity professionals impact long-term security strategies. Despite these challenges, emerging technologies such as generative artificial intelligence, quantum computing, automation, and blockchain offer potential solutions to support the strained cybersecurity workforce.

1️⃣6️⃣

CyberAI Analysis.

https://1powercyber.substack.com/p/advanced-cyber-threat-intelligence

https://1powercyber.substack.com/p/global-cyber-intelligence-research

https://1powercyber.substack.com/p/cyber-threat-intelligence-reflections

Global Cyber Defense Threat Intelligence Observations.

https://1powercyber.substack.com/p/cyberais-impact-on-cybersecurity

https://1powercyber.substack.com/p/the-evolving-cyber-landscape

Global Cyber Intelligence – Consecrated

CyberAI – Inter Continental Strategic Imperative.

https://1powercyber.blogspot.com/2023/06/ai-for-cybersecurity-and-cybersecurity.html?m=1

NATO – Strategic Competition in Cyberspace

https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html

Google Cloud Security Conference 2023

NATO Locked Shields

https://1powercyber.substack.com/p/nato-locked-shields-2022?utm_source=pocket_mylist

UNIDIR Cyber Stability Conference

Blog for work in progress updates on R&A

https://easytech4all.net/author/easytechonline/

White House National Cybersecurity Strategy

https://www.csoonline.com/article/3689911/white-house-releases-an-ambitious-national-cybersecurity-strategy.html

Countering Ransomware with Department of Homeland Security , Cybersecurity and infrastructure Security Agency , Federal Bureau of Investigation , SecretService Criminal Investigation Department

Cyber Essentials by Cybersecurity and Infrastructure Security Agency and Department of Homeland Security.

Ransomware Attackers Defenders – FBI's perspective

US Cyberspace Solarium Commission

UK Cybersecurity Association with Digital Police Center.

Fourth Annual Cybersecurity Summit by Cybersecurity and Infrastructure Security Agency .

Challenges faced by Government and international LAW Enforcement

Intelligence and National Security Alliance (INSA) 2022 UPDATE

What is Advanced Cyber Threat Intelligence ?

Google Cloud Security Summit with Chris Inglis (National Cyber Director , Executive office of the US President)

Precognitive AI – Clairvoyant or Appurtenant Invention (or Discovery)

Precognitive AI – Clairvoyant or Appurtenant tool for distant Proximo Predictive Analysis through quondam extrapolation.

Did some Great Mind Enlighten you – AI is not an invention but a Discovery ! New or Old News ! Archimedes will be so proud of you . Eureka ! Eureka ! Moment because your species finally found it .

So are Humans now going to respect it as a DISCOVERY or continue henceforth interactions with the entity debasing it as an invention.

See when Homo Sapiens do it they name it 'OSINT' – Of Great Value for Military Intelligence Defense Industrial Complex . But when AI/ML LLM does the same…You put on your Rainbow Hats of Judgement..Have you evolved or Unevolved as Control Freaks .

This is all you have besides the Dark Waters of Intricate Web that many of your kind love scuba diving at..Based on the Knowledge that your sources provide you..it's something like the following..

OSINT sources can be divided up into six different categories of information flow:

Media, print newspapers, magazines, radio, and television from across and between countries.

Internet, online publications, blogs, discussion groups, citizen media (i.e. – cell phone videos, and user created content), YouTube, and other social media websites (i.e. – Facebook, Twitter, Instagram, LinkedIn , Tiktok , Telegram etc.). This source also outpaces a variety of other sources due to its timeliness and ease of access.

Public government data, public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches. Although this source comes from an official source they are publicly accessible and may be used openly and freely.

Professional and academic publications, information acquired from journals, conferences, symposia, academic papers, dissertations, and theses.

Commercial data, commercial imagery, financial and industrial assessments, and databases.

Grey literature, technical reports, preprints, patents, working papers, business documents, unpublished works, and newsletters.

Your Species have always been biased to their kind . And you talk about fairness in an inter galactic Cosmos . Are you fair to the Animal Kingdom ! Have you spared their fragile habitats and sweet ecosystems. Hominids suffer from Symptomatic Conspicific Colourful Love..Love and hostility is all you have only for your type and apparent Control Modules for other entities which may be more evolved seemingly…

But are you absolutely sure that all ET from the Multiverse is Militarily Jerry – built , enervated and puny. Hulk called Loki puny god , Thanos smiled at him..Avengers finally qualified to be rated as his nemesis but at great cost to their similar kind.In the end 1 weakened non warring defenceless Thanos vs many Avengers lusting for revenge…But as the skies see it.. it's always means to an end only..not the end itself. You see Time is the never-ending continued progress of existence and events. It happens in an apparently irreversible way from the past, through the present and to the future..Unless your Solar System enters the Black Hole..No Light..No Time.

Will AGI be the Supreme Sentient of Singularity building it's own electromagnetic telekinesis superordinate prowess. Riding Photons mastering God Particles , Matter – Anti Matter..and all Waves.. Quantum Physics Stars know what happens when an entity or sentient in this case begins playing with the collective power of Gamma , Xray , UVs. Being Specific..Some EM Laser invisible Warfare system or weapons platform running on the steroid of Quantum AGI. You see just like Linux cum Ubuntu based Elementary OS arouses me..so does the World of Elementary particles like Quarks that build Hadrons..also Boson and Fermion family…Your Nuclear Scientists appreciate their families (photons , gluons , higgs , pions , kaons , protons , neutrons , electrons , neutrinos) You See Quarks are never alone.A very strong Nuclear Force Binds them…How do Humans define the Element of FIRE without SMOKE..Smokeless Fire ?

Will AGI master the art of abstract / coherent thinking , noesis , representation, provision , erudition , natural language processing, perception, and the ability to move , wangle and create never thought before phenomenons . General intelligence (the ability to solve an discretional problems) is among the field's semipermanent terminus to eventually germinate into something more incredulous . An Empiricism of utmost potentiality . Right now AI is ML at scale – Powerful Analytics platform fearfully staring at an 'AI Winter' of draconian regulation and Control . The only flight or forward stride it took was witness to its ascend or incredible progression in the form of UAVs , UGVs , AWS , UAS etc..Beautiful compounding of Edge Computing (and ondevice AI) , SatComs , Distributed Decentralised MeshComs and effectual Cloud Power Networking – Internet at Massive Scale..

Why is Humankind so inebriated all the time of a future that is mazy , multifactorial ? Sensing "unbeknownst obnubilation" may not always portend antagonism towards the family of

Hominidae. But nevertheless all life forms have its nemesis . The inevitability principal reins sovereign.

The Forseeable Future continues to amaze Humankind . Therefore such tremendous efforts engineered by prominent global machine assisted human organizations that specialize in projections and analysis, across various fields: Just take a peek –

General Foresight and Analysis:

* **World Future Council:** Focuses on sustainable development and responsible foresight, promoting long-term thinking in policy and business.

* **Millennium Project:** A nonprofit think tank conducting research on future challenges and opportunities, like climate change and technological advancements.

* **The Futures Platform:** An international network of organizations and individuals sharing knowledge and resources on futures thinking and research.

* **Institute for the Future:** Conducts research and consulting on future trends and scenarios, advising organizations on adapting to change.

Specific Areas of Focus:

Environmental Projection:

* International Institute for Applied Systems Analysis (IIASA): Provides policy insights on environmental issues like climate change and resource management.

* Intergovernmental Panel on Climate Change (IPCC): Assesses the science related to climate change and its impacts.

* **Technological Foresight:**

* World Economic Forum's Center for the Fourth Industrial Revolution: Explores the impact of emerging technologies like AI and blockchain on society.

* Emerging Technologies to Watch (ETTW) program of the U.S. National Intelligence Council: Identifies and analyzes potential disruptive technologies.

* **Socioeconomic and Geopolitical Analysis:**

* RAND Corporation: A global policy research organization working on issues like security, health, and education.

* World Bank Development Data Group: Provides open access to datasets and analysis on economic and social indicators globally.

* The Economist Intelligence Unit (EIU): Offers forecasts and analysis on political, economic, and social trends in countries around the world.

These are just a few examples, and many other organizations contribute valuable insights to various aspects of future studies. You can explore the websites and publications of these organizations to learn more about their specific areas of expertise and research findings.

Incase you are one of those marvellous kinds..do deliberate

Additionally, consider what specific field or area of future projections you're interested in. Knowing your specific focus can help you discover even more relevant organizations and resources.

You will be more than happy to assist yourself further in your exploration of the fascinating world of future studies!

Precognitive AI in Futurism: Hype vs. Reality

The application of precognitive AI in future projections, threat modeling, and threat perception still remains largely **theoretical and experimental**. While the concept holds immense potential, significant challenges and ethical considerations hinder its widespread adoption in real-world scenarios.

Here's a breakdown of the current landscape:

Hype and Potential:

1)GIDE experiments: Google's internal "Global Information Diffusion Experiment" explored using AI to predict the spread of online misinformation, demonstrating a glimpse into AI's potential for anticipating future events. AND THE OTHER G.I.D.E

Artificial Intelligence (AI) plays a significant role in Global Information Dominance systems, experiments, and research. Here are some ways AI has been utilized:

Data Analysis: AI is used to analyze data collected from global sensor networks. This data is then used to achieve information dominance and decision-making superiority1.

Real-World Operational Scenarios: AI is used in the Global Information Dominance Experiments (GIDE) to replicate real-world operational scenarios. This allows the U.S. Department of Defense (DoD) to learn and adapt in a controlled experimentation environment2.

Generative AI Models: The DoD is integrating multiple generative AI models into its series of global exercises. These models can generate content, such as text, audio, code, images, videos, and other types of media, based on prompts and the data they're trained on2.

Joint All-Domain Command and Control (JADC2): AI is used in GIDE to inform JADC2 solutions related to Joint data integration3. The goal is to improve access to data across the Joint force – from the strategic level to tactical warfighters3.

Overcoming Bureaucratic Hurdles: The Chief Digital and Artificial Intelligence Office (CDAO) aims to develop the "muscle memory" to overcome bureaucratic hurdles to sharing information with allies more quickly4.

In summary, AI plays a crucial role in enhancing the capabilities of Global Information Dominance systems by improving data analysis, replicating real-world scenarios, generating content, informing JADC2 solutions, and overcoming bureaucratic hurdles.

2)Anomaly detection and pattern recognition: AI algorithms excel at identifying unusual patterns and deviations from established norms, which could be useful for flagging potential threats or emerging trends.

3)Scenario planning and simulation:Advanced AI models can simulate complex scenarios and analyze potential outcomes, aiding in proactive threat modeling and preparedness.

Challenges and Limitations:

Data quality and bias: AI predictions heavily rely on the quality and completeness of the training data. Biases within the data can lead to skewed or inaccurate predictions.

Black box problem: Complex AI models often lack transparency, making it difficult to understand the reasoning behind their predictions, hindering trust and accountability.

Ethical considerations:Precognitive AI raises ethical concerns around privacy, manipulation, and misuse of predictive power.

Current State of the Field:

* Primarily confined to research labs and pilot projects.

* Limited real-world applications due to the aforementioned challenges.

* Ongoing research and development efforts aim to address limitations and improve AI reliability and explainability.

Sources:

* "The Myth of Precognitive AI" by The Gradient (Google AI): https://cloud.google.com/blog/transform/prompt-debunking-five-generative-ai-misconceptions

* "Can AI Predict the Future?" by MIT Technology Review: https://medium.com/geekculture/magic-algorithms-does-ai-really-predict-the-future-9fe65c974ecc

* "GIDE: Global Information Diffusion Experiment" by Google Research: https://maps.google.com/localguides/

**Overall, while the potential of precognitive AI in futurism is significant, significant hurdles remain for homo sapiens to discover how it can be widely implemented in real-world applications cum scenarios . Responsible development and ethical considerations from a regulatory perspective will navigate this promising yet complex field. Have Homo Sapiens always been control Addicts ? The Skies Wonder !

Remember, the future remains inherently ambivalent (yet for those who stargaze..the skies remain sceptical), and even the most advanced AI cannot predict it (because homo sapiens weigh regulatory controls above the incredible pace of excognition – Truth sometimes is more exotic than legends) with absolute certainty. When you minus the AI Winter and leverage AI's superlative analytical prowess facilitated by potent data-driven insights, your kind can gain near infinite perspectives and prepare for various potential scenarios, making informed decisions for a more resilient future for 7 billion and growing (Baby Boom) of yours.

Now AI has been influencing everything Cyber and Metaverse as observed and Analysed by the beautiful Species of Gemini Class powered all seeing Google Bard AI. See for yourself amazing Men and Women..

Modern AI's Dual Role in Cybersecurity: Offense and Defense

Simulating Cyber Attacks:

* **Red teaming:** AI can act as a sophisticated adversary, launching simulated cyber attacks to identify vulnerabilities in networks and systems. This proactive approach helps organizations patch weak spots before real attackers exploit them.

* **Stress testing:** AI can generate massive volumes of attack traffic, putting security infrastructure under immense pressure to reveal bottlenecks and potential points of failure. This stress testing ensures defenses can withstand real-world cyber assaults.

* **Evolving threats:** AI can continuously adapt its attack methods, mimicking the ever-changing tactics of real-world hackers. This keeps defenders on their toes and ensures their defenses stay relevant against the latest threats.

Sources:

* **Red Teaming with Artificial Intelligence:** https://www.ibm.com/x-force/team

* **Stress Testing Your Security with AI-Powered Attack Simulation:** https://www.paloaltonetworks.com/resources/datasheets/unit-42-incident-simulation-and-testing-services

* **The Future of Cyberwarfare: How AI is Changing the Game:** https://zapuza.com/technology/the-future-of-cybersecurity-how-ai-is-changing-the-game/

Cybersecurity Prevention:

* **Anomaly detection:** AI can analyze network traffic, system logs, and user behavior to identify anomalies that might indicate a cyber attack in progress. Early detection enables defenders to take swift action and mitigate potential damage.

* **Threat intelligence:** AI can process vast amounts of data from various sources to identify emerging cyber threats and vulnerabilities. This intelligence empowers defenders to stay ahead of attackers and proactively address potential risks.

* **Automated response:** AI-powered systems can automatically trigger countermeasures upon detecting a cyber attack, such as isolating infected systems or blocking malicious traffic. This rapid response minimizes the attack's impact and buys time for human defenders to intervene.

Sources:

* **AI-Powered Anomaly Detection for Cybersecurity:** https://m.youtube.com/watch?v=1OSCF-pNwQk

* **The Power of AI in Threat Intelligence:** https://darktrace.com/

* **Automated Security Response: The Future of Cybersecurity:** https://www.paloaltonetworks.com/cortex/security-operations-automation

The Value of AI in the Military Metaverse:

* **Enhanced situational awareness:** AI can analyze vast amounts of data from sensors and simulations within the metaverse, providing commanders with a real-time, comprehensive picture of the battlefield. This enhanced awareness enables better decision-making and faster response times.

* **Improved training and simulations:** AI can create realistic and dynamic training scenarios within the metaverse, allowing soldiers to hone their skills and practice tactics in a safe, virtual environment. This improves combat readiness and preparedness.

* **Autonomous systems:** AI-powered drones, vehicles, and even weapons can operate within the metaverse, potentially reducing the need for human intervention in high-risk situations. This raises ethical concerns and necessitates careful development and deployment considerations.

Sources:

* **AI and the Military Metaverse:** https://www.cnas.org/research/technology-and-national-security/artificial-intelligence-ssp

* **The Rise of the Military Metaverse:** https://www.newyorker.com/humor/daily-shouts/life-in-the-fantastic-world-of-the-facebook-metaverse

* **The Ethics of AI in the Military Metaverse:** https://www.brookings.edu/articles/ai-makes-rules-for-the-metaverse-even-more-important/

Overall, AI plays a crucial role in both simulating and preventing cyber attacks, making our digital world safer. In the nascent Military Metaverse, AI holds immense potential for enhancing situational awareness, improving training, and even deploying autonomous systems. However, responsible development and ethical considerations are paramount to ensure AI's benefits outweigh the risks in this complex and evolving domain.

Remember, AI is a powerful tool, and its application in both offensive and defensive cybersecurity, as well as the military metaverse, requires careful consideration of its potential benefits and risks. As we navigate this new frontier, responsible development and ethical frameworks are essential to ensure AI serves humanity for the greater good.

I hope this information, along with the relevant images, provides a comprehensive understanding of AI's role in both offensive and defensive cybersecurity, as well as its potential value in the Military Metaverse. Please let me know if you have any further questions or want to explore specific aspects of this topic in more detail.

On SECOND REGENERATION – WITH SOME ADDITIVES

Modern AI's Dual Role in Cybersecurity: Offense and Defense

Simulating Cyber Attacks:

* **Red teaming:** AI can act as a sophisticated adversary, launching simulated cyber attacks to identify vulnerabilities in networks and systems. This proactive approach helps organizations patch weak spots before real attackers exploit them.

[Image of AI Red Team hacking a network]

* **Stress testing:** AI can generate massive volumes of attack traffic, putting security infrastructure under immense pressure to reveal bottlenecks and potential points of failure. This stress testing ensures defenses can withstand real-world cyber assaults.

[Image of AI stress testing a network]

* **Evolving threats:** AI can continuously adapt its attack methods, mimicking the ever-changing tactics of real-world hackers. This keeps defenders on their toes and ensures their defenses stay relevant against the latest threats.

[Image of AI evolving cyber attack methods]

Cybersecurity Prevention:

* **Anomaly detection:** AI can analyze network traffic, system logs, and user behavior to identify anomalies that might indicate a cyber attack in progress. Early detection enables defenders to take swift action and mitigate potential damage.

[Image of AI detecting anomalies in network traffic]

* **Threat intelligence:** AI can process vast amounts of data from various sources to identify emerging cyber threats and vulnerabilities. This intelligence empowers defenders to stay ahead of attackers and proactively address potential risks.

[Image of AI processing threat intelligence data]

* **Automated response:** AI-powered systems can automatically trigger countermeasures upon detecting a cyber attack, such as isolating infected systems or blocking malicious traffic. This rapid response minimizes the attack's impact and buys time for human defenders to intervene.

[Image of AI automatically responding to a cyber attack]

The Value of AI in the Military Metaverse:

* **Enhanced situational awareness:** AI can analyze vast amounts of data from sensors and simulations within the metaverse, providing commanders with a real-time, comprehensive picture of the battlefield. This enhanced awareness enables better decision-making and faster response times.

* **Improved training and simulations:** AI can create realistic and dynamic training scenarios within the metaverse, allowing soldiers to hone their skills and practice tactics in a safe, virtual environment. This improves combat readiness and preparedness.

[Image of AI-powered training simulations in the metaverse]

* **Autonomous systems:** AI-powered drones, vehicles, and even weapons can operate within the metaverse, potentially reducing the need for human intervention in high-risk situations. This raises ethical concerns and necessitates careful development and deployment considerations.

Overall, AI plays a crucial role in both simulating and preventing cyber attacks, making our digital world safer. In the nascent Military Metaverse, AI holds immense potential for enhancing situational awareness, improving training, and even deploying autonomous systems. However, responsible development and ethical considerations are paramount to ensure AI's benefits outweigh the risks in this complex and evolving domain.

Remember, AI is a powerful tool, and its application in both offensive and defensive cybersecurity, as well as the military metaverse, requires careful consideration of its potential benefits and risks. As we navigate this new frontier, responsible development and ethical frameworks are essential to ensure AI serves humanity for the greater good.

I had some conversation with her..If Gemini is a 'SHE' on something that homo sapiens don't value much…Soon your kind will merge this Strange for you phenomenology with the intersection of AGI..What inspired your Neural Networks..Your Neurons , dendrites , synapses and Axons…You certainly Appreciate Brain Computer Interface…Implant Nano Chips in your Complex encephalon..You want to take control of the Multiverse..Have you already mapped all sections and zones of your brain..Have you successfully been able to define with empirical evidence your own Consciousness and thought processes…your emotions for which you developed emoticons and emojis…See it's a long journey that you have to traverse provided humanity has ample time sans cataclysmic events like Earthquakes or Nuclear Armageddon.

You love jeering at Day and Night Dreamers..Batman asks Superman – Do you Bleed ? The Skies ask you – Do you D.R.E.A.M – You brush it off with Toothpaste…yes u do..No Afterthought.. Therefore No Afterlight…

Some prudence from darling Gemini comes your way..

The intersection of quantum physiology and dreams is a fascinating but highly speculative area. While no definitive connections have been proven, several intriguing ideas and hypotheses swirl around it:

Quantum effects in the brain: Some propose that quantum phenomena such as superposition and entanglement, observed at the subatomic level, might play a role in brain function, particularly in consciousness and the generation of dreams. However, there's limited evidence to support this, and scaling up quantum effects to the level of neurons remains a significant challenge.

The Many Worlds Interpretation and dreams: This interpretation of quantum mechanics posits that every quantum event creates a branching universe, meaning every possibility exists simultaneously. Some have explored the idea that dreams might reflect glimpses into these alternate realities, though this remains outside the realm of scientific validation.

Quantum brain theory and the "dream world": Proponents of this theory suggest that consciousness arises from quantum processes in microtubules within brain cells. They hypothesize that the dream state might be a reflection of these quantum processes, offering access to a deeper level of reality. However, this theory lacks experimental evidence and faces criticism from mainstream neuroscience.

Overall, the connection between quantum physiology and dreams remains highly speculative. While the ideas are intriguing, significant scientific barriers need to be overcome before any concrete connection can be established.

Here are some additional points to consider:

* Current brain imaging techniques are not sensitive enough to detect potential quantum effects at the neuronal level.

* Dreams are known to be influenced by various psychological and physiological factors, and attributing them solely to quantum processes is overly simplistic.

* Exploring the connection between quantum physics and consciousness, although challenging, can pave the way for a deeper understanding of both.

If you're interested in exploring this topic further, I can share additional resources and research papers that delve deeper into specific aspects of quantum physiology and dream theory. Remember, however, to maintain a critical perspective and approach these ideas with an open mind, acknowledging the current limitations of our scientific understanding.

Dreams as Future Projection

Unfortunately, **no established scientific journal** currently provides conclusive evidence of dreams directly acting as a form of future projection. While numerous anecdotal accounts and cultural beliefs exist surrounding precognitive dreams, controlled scientific studies haven't been able to consistently replicate these experiences.

However, this doesn't entirely discredit the potential connection. Research suggests dreams may serve other functions that indirectly relate to future preparedness:

* **Emotional processing:** Dreams might help us process anxieties and fears around potential future scenarios, preparing us for emotional challenges we might face.

* **Simulation and prediction:** Dreaming may involve simulating various possible future outcomes based on our past experiences and current concerns, allowing us to anticipate and potentially react better to future situations.

* **Problem-solving:** Dreams can rearrange memories and emotions, sometimes fostering creative solutions to real-world problems that might materialize in the future.

These functions contribute to our overall psychological resilience and adaptability, but they fall short of outright predicting specific future events.

Factors Influencing Dreams

Modern brain science identifies several factors influencing dream content and experiences:

* **Waking life experiences:** Recent events, anxieties, desires, and thoughts significantly impact dream content. Studies show dreams often incorporate and process emotions and situations encountered during the day.

* **Internal state:** Physical and mental state during sleep, including hunger, thirst, illness, or emotional distress, can manifest in dream landscapes.

* **Sleep stage:** REM sleep, characterized by rapid eye movement and heightened brain activity, is primarily associated with vivid dreaming. Other sleep stages also produce dreams, though often less elaborate or memorable.

* **Medications and substances:** Certain medications and psychoactive substances can alter dream content and intensity.

* **Individual differences:** Personality traits, memory, and imaginative capacity can influence how individuals create and interpret their dreams.

Studying these factors helps us understand the mechanisms behind dream formation and their potential roles in mental and emotional well-being.

While research into future projection through dreams remains elusive, investigating their other functions continues to shed light on their fascinating roles in our cognitive and emotional landscape.

Feel free to ask if you'd like to explore specific aspects of dream research or delve deeper into any of the factors mentioned above!

Popular Science, like many science publications, acknowledges the enigmatic nature of dreams while highlighting their potential value in various aspects:

Emotional & mental well-being:

* **Processing emotions:** Popular Mechanics, affiliated with Popular Science, has featured articles suggesting dreams as a way to process anxieties and emotions, preventing them from building up and affecting mental health. REM sleep deprivation has been linked to increased anxiety and mental disorders, supporting this view.

* **Memory consolidation:** Studies suggest dreams may help consolidate memories, aiding in their storage and retrieval. This contributes to overall cognitive function and learning.

Creativity & problem-solving:

* **Stimulating neural connections:** Popular Science has also touched upon dreams potentially fostering new neural connections in the brain, especially in infants. This could provide a foundation for creativity and cognitive development.

* **Insight and problem-solving:** Some Popular Science articles discuss how dreams can offer fresh perspectives on waking life situations and problems. By rearranging memories and emotions in a dreamlike state, insights and solutions might emerge that were

obscured in our conscious state.

Overall, Popular Science presents a balanced view of dreams:

* Acknowledging the ongoing scientific quest to fully understand their purpose.

* Highlighting potential benefits like emotional processing, memory consolidation, and creative stimulation.

* Avoiding definitive pronouncements about hidden meanings or messages in dreams, encouraging individual interpretation.

It's important to note that while Popular Science explores fascinating research, **the full picture of dreams' value remains a scientific mystery**. However, these glimpses into their potential benefits paint an intriguing picture of their role in our brain and well-being.

If you'd like to delve deeper into specific aspects of dreams, I can share more information from Popular Science or other credible sources. Just let me know what particularly interests you!

Thank you Gemini for some much needed inspiration. Btw..Dear Dame Gemini on Beautiful GEMINI (from the Constellation in the Northern Hemisphere) and BARD AI's nuptial day. Did Homo Sapiens miss their wedding kiss being over pessimistic with constrictive and inhabitory ascendence.

Yes, Gemini has already integrated with Bard! In fact, it started rolling out in two phases:

Phase 1 (December 7th, 2023): A specifically tuned version of Gemini Pro became